# Technologies de filtrage de contenu et fournisseurs de services Internet

## *permettant à l'utilisateur de faire des choix*

**Michael Shepherd et Carolyn Watters**[1]

**Laboratoire de filtrage de l'information diffusée sur le Web**
**(Web Information Filtering Lab)**
**Faculty of Computer Science**
**Dalhousie University**
**6050 University Avenue**
**Halifax (Nouvelle-Écosse) Canada B3H 1W5**
**{shepherd | watters}@cs.dal.ca**

**22 mars 2000**

[1] Assistés de Margo Boyd, adjointe à la recherche

## Table des matières

Résumé ..... 3
1. Introduction ..... 7
2. Plan de classification des technologies de filtrage ..... 10
  2.1. Plan à deux couches ..... 10
    2.1.1. Technologies de base ..... 11
    2.1.2. Applications de filtrage ..... 12
  2.2. Modes d'accès ..... 14
3. Description des technologies de filtrage ..... 17
  3.1 Technologies de base ..... 17
    3.1.1 Systèmes d'étiquetage de sites ..... 17
    3.1.2 Listes d'URL ..... 26
    3.1.3 Analyse automatique du texte ..... 28
    3.1.4 Méthodes de contrôle des autorisations ..... 34
    3.1.5 Repérage des activités ..... 35
  3.2 Niveau applications ..... 36
    3.2.1 Applications de navigation pour enfants ..... 36
    3.2.2 Moteurs de recherche et portails axés sur les intérêts des enfants ..... 36
    3.2.3 Applications mandataires ..... 37
    3.2.4 Applications de surveillance des activités ..... 40
    3.2.5 Applications limitant l'accès aux données ..... 40
    3.2.6 Applications autres que des applications HTTP ..... 41
4. Évaluation des types de technologies de filtrage ..... 43
  4.1 Technologies de base ..... 43
    4.1.1 Étiquetage de sites ..... 43
    4.1.2 Listes d'URL ..... 44
    4.1.3 Analyse automatique du texte ..... 44
    4.1.4 Méthodes d'autorisation ..... 45
    4.1.5. Repérage des activités ..... 46
  4.2 Applications ..... 47
    4.2.1 Navigateurs pour enfants ..... 47
    4.2.2. Portails et moteurs de recherche axés sur les intérêts des enfants ..... 47
    4.2.3. Applications mandataires ..... 47
    4.2.4. Applications d'autorisation d'accès ..... 48
    4.2.5. Moniteurs d'activités ..... 48
    4.2.6. Filtage dans le cas des applications non HTTP ..... 49
5. Site où s'opère le filtrage ..... 50
  5.1 Mécanismes autonomes (ordinateur client) ..... 50
  5.2 Mécanismes du FSI ..... 51
6. Résumé et recommandations ..... 53
Annexe ..... 56
  Exemples de logiciels de filtrage ..... 56

**Résumé**

Le présent rapport traite des mécanismes que les fournisseurs de services Internet (FSI) ont le *choix* d'offrir et que les utilisateurs peuvent eux-mêmes *choisir* d'utiliser pour filtrer le contenu mis à leur disposition sur Internet et en autoriser l'accès. Nous y décrivons uniquement les mécanismes de filtrage et ne fournissons donc pas de ligne directrice ni de conseils ou de recommandations d'ordre juridique. Cette étude a été commissionée par Industrie Canada dans le but de promouvoir le développement et l'utilisation de technologies permettant aux utilisateurs de l'Internet de faire des choix avisés sur les contenus auxquels ils ont accée sur le réseau Internet.

*Classification des mécanismes*

Les mécanismes de filtrage se divisent en deux parties : mécanismes au niveau des applications et technologies de base sous-jacentes. Les technologies de base se classifient comme suit :

- **Étiquetage des sites.** L'étiquetage désigne les mécanismes utilisés pour attribuer à des URL et à des pages Web précises des étiquettes liées au contenu. L'URL (Universal Resource Locator) décrit l'emplacement d'une page Web particulière. Les protocoles d'évaluation individuels sont généralement séparés des produits ou des applications qui les utilisent. En règle générale, les étiquettes qui sont attribuées peuvent être enregistrées dans la page Web ou séparément, dans une base de données. Ces étiquettes peuvent être attribuées selon une autoévaluation, selon l'évaluation de services indépendants ou encore selon l'évaluation de groupes d'utilisateurs concernés[2].
- **Listes de sites appropriés ou de sites inappropriés (listes « blanches » et listes « noires »).** La méthode de filtrage la plus courante consiste à utiliser des listes d'URL acceptables et/ou inacceptables. Les listes « blanches » servent à définir un domaine de sites Web « sûrs », dans les limites duquel les utilisateurs peuvent naviguer. Ce genre de liste exige normalement de rechercher et de sélectionner des sites qui sont approuvés par le fournisseur de la liste. Les listes « noires », elles, sont des listes compilées d'adresses URL pour lesquelles les demandes ne seront pas honorées. Ces listes sont compilées à titre de service par des utilisateurs individuels ou par des groupes d'évaluateurs.
- **Analyse automatique du texte.** Une autre façon d'analyser un site Web consiste à utiliser un logiciel qui analyse le texte du site pour en déterminer la pertinence ou la convenance. Les utilisateurs ou les groupes d'utilisateurs ont des profils d'intérêts (positifs et/ou négatifs), composés de mots-clés et d'expressions, qui servent justement à établir cette pertinence. Presque tout le filtrage basé sur le contenu utilise une forme de couplage de mots-clés, les

[2] Balkin, J., B.Noveck et K.Roosevelt. 1999. Filtering the Internet: A best practices model. In *Protecting our children on the Internet: towards a new culture of responsibility.* Bertelsmann Foundation Pub. [www.stiftung.Bertelsmann.de/internetcontent/english/frameset_home.htm]

mots-clés d'un profil d'intérêts étant comparés avec les mots-clés du contenu d'une page Web donnée. L'analyse du texte est également utilisée pour sélectionner des termes de recherche à partir des requêtes.

- **Autorisation.** Le chiffrement, la protection par mot de passe et la validation des cartes de crédit sont des méthodes utilisées pour certifier qu'un utilisateur a l'autorisation d'accéder à certains services ou à certaines données.
- **Repérage des activités.** L'utilisation qui est faite d'Internet peut être retracée à l'aide des fichiers journaux du serveur et d'autres journaux de données. Ces fichiers enregistrent les détails de tous les accès au Web et peuvent servir à analyser les activités liées au Web.

Les applications de filtrage qui sont basées sur ces technologies ont été classifiées comme suit :

- **Navigateurs pour enfants.** Il est possible de créer des navigateurs à l'intention des jeunes utilisateurs. Ces navigateurs peuvent offrir des stratégies de recherche simplifiées et des graphiques plus conviviaux, supprimer les annonces publicitaires et fournir des fonctions de filtrage et des domaines de recherche sûre de façon transparente.
- **Moteurs de recherche et portails axés sur les intérêts des enfants**. L'idée est d'utiliser, dans ces deux cas, une passerelle de tiers qui donne accès au contenu du Web. Les portails conçus pour les enfants sont des sites d'accès au Web qui essaient de fournir un domaine de sites sûrs que l'utilisateur peut explorer. Du moment qu'il passe par le portail, l'utilisateur ne peut visualiser qu'un ensemble de domaines présélectionnés du Web.
- **Applications mandataires.** Les applications mandataires sont des logiciels au niveau de l'FSI qui font office d'intermédiaire entre le client ou le navigateur et Internet. Un logiciel d'application peut être ajouté aux modules mandataires du serveur, et ce, pour permettre l'analyse du texte et la comparaison des listes d'URL à chaque demande et réponse du navigateur Internet.
- **Moniteurs d'activité**. Plutôt que de limiter ou de contrôler l'accès aux sites Web de façon proactive, ces applications surveillent et enregistrent les activités effectuées sur Internet pour que les parents puissent les examiner ultérieurement.
- **Applications limitant l'accès aux données**. Les applications qui résident sur le site hôte peuvent être élaborées de façon à ne permettre qu'aux utilisateurs autorisés d'accéder aux données ou aux services offerts sur ce site. Ces applications peuvent chiffrer les données de sorte que seuls les utilisateurs autorisés puissent les déchiffrer et les visualiser.
- **Applications autres que des applications HTTP.** Outre les applications qui limitent l'accès aux pages Web, il est possible de créer des applications à l'aide de ces technologies de base pour filtrer le contenu du courrier électronique et pour contrôler l'accès aux sites FTP, aux hôtes Telnet, aux groupes de discussion et de bavardage et aux groupes de nouvelles.

*Possibilités qu'offrent les technologies de base*

Toutes ces technologies de base ont un rôle à jouer dans les mécanismes de filtrage conçus pour le Web. Aucune d'elles ne fournit cependant de solution à long terme. Les systèmes devront donc les combiner de façon novatrice pour offrir des solutions efficaces. Soulignons particulièrement ceci :

- Les systèmes d'étiquetage de site sont les systèmes les plus souples et sont peut-être les plus prometteurs. Les étiquettes peuvent être attribuées par le fournisseur de contenu, par des services d'évaluation indépendants, ainsi que par des groupes d'utilisateurs ou des utilisateurs individuels. Il revient à l'FSI et/ou au client d'utiliser les étiquettes qui ont été attribuées.
- L'utilisation de listes d'URL constitue la méthode la plus efficace pour contrôler les domaines d'accès. Cette méthode convient particulièrement bien pour créer des listes de sites pour enfants. Toutefois, l'utilisation de listes n'offre pas toute la souplesse des étiquettes et le Web s'agrandit si rapidement qu'il est très difficile de garder des listes à jour.
- L'analyse automatique précise du contenu des sites Web est problématique dans le meilleur des cas, compte tenu des fantaisies du langage naturel, des problèmes de filtrage des divers langages et de la difficulté qu'il y a à déterminer le contenu des graphiques et des images. Toutefois, l'utilisation de cette technologie pour *faciliter* l'étiquetage des sites d'après les méthodes de catégorisation de texte s'avère d'une certaine manière prometteuse.
- Le droit d'accès peut être efficace comme filtre inverse, car il limite l'accès à un site donné.
- La méthode de repérage des activités ne permet que de surveiller ce qui a été fait; elle ne permet pas de filtrer quoi que ce soit.

Même si on considère qu'ils ne font pas partie des technologies de base, les robots Web peuvent faire office d'agents d'évaluation qui classent les sites de façon proactive d'après des algorithmes d'analyse de contenu. Bien qu'elle n'ait pas encore fait preuve de grande précision, cette méthode mérite d'être améliorée.

Notons qu'aucune des technologies mentionnées n'est efficace à cent pour cent et que le contenu du Web est de par nature très volatile. Pour augmenter l'efficacité de ces technologies, il faut les combiner et les utiliser en couches, à la fois au niveau du FSI et au niveau du client. Étant donné que les applications et les technologies de base s'emploient en combinaison et que la plupart peuvent être utilisées au site du FSI, à celui du client ou aux deux, nous n'avons aucune recommandation particulière à faire quant aux meilleures méthodes ou aux meilleurs sites d'utilisation.

Les secteurs qui offrent les plus grandes possibilités et sur lesquels on devrait axer les futurs travaux sont les suivants :

- Développement d'architectures qui combinent divers mécanismes permettant de travailler en collaboration ou constituant des couches d'architecture. On

pourrait par exemple avoir des étiquettes gérées par un bureau d'étiquettes (Label Bureau), avec des listes gérées par le FSI, l'analyse du contenu étant gérée au niveau du client.

- Recherches plus approfondies en ce qui concerne les robots et les agents Web pour permettre la catégorisation proactive des sites Web.
- Développement d'architectures gérant le filtrage coopératif pour des groupes d'utilisateurs.

Alors que pratiquement toutes les méthodes étudiées dans ce rapport peuvent être mises en œuvre par un FSI, il importe que le filtrage soit transparent pour l'utilisateur. L'utilisateur doit savoir à quel moment le filtrage est en place ou à quelle étape il a eu lieu. Pour que la méthode soit efficace, voici ce qui importe :

- L'utilisateur doit savoir à quelle étape le contenu a été filtré et pourquoi il a été filtré.
- L'utilisateur doit connaître les critères de filtrage, c'est-à-dire ce qui figure sur la liste ou dans le filtre.

Compte tenu de la nature dynamique du Web, il faudra axer les efforts, de façon concertée et soutenue, sur le développement, l'évaluation et la maintenance de mécanismes de filtrage et de contrôle d'accès, et ce, à tous les niveaux - gouvernement, collectivité, FSI et utilisateurs individuels.

## 1. Introduction

Le présent rapport traite des mécanismes que les fournisseurs de services Internet (FSI) ont le *choix* d'offrir et que les utilisateurs peuvent eux-mêmes *choisir* d'utiliser pour filtrer le contenu mis à leur dFSIosition sur Internet et en autoriser l'accès. Nous y décrivons uniquement les mécanismes de filtrage et ne fournissons donc pas de ligne directrice ni de conseils ou de recommandations d'ordre juridique. Cette étude a été commissionée par Industrie Canada dans le but de promouvoir le développement et l'utilisation de technologies permettant aux utilisateurs de l'Internet de faire des choix avisés sur les contenus auxquels ils ont accée sur le réseau Internet.

Internet aura bientôt, au Canada, le statut de mass media et il pose à ce titre certains des problèmes qui se sont posés lorsque les médias traditionnels comme la télévision ont envahi la vie moderne. Ce qui est particulier à Internet, c'est qu'il offre un moyen par lequel des informations choquantes et répréhensibles peuvent pénétrer dans des millions de foyers canadiens. La facilité d'accès à toute une variété de contenus que certaines personnes jugent répréhensibles préoccupe grandement le public. En fait, on reconnaît de plus en plus que l'existence de contenu offensant en ligne - bien qu'il ne s'agisse que d'une très petite partie du contenu disponible en ligne - pourrait constituer une barrière importante à l'expansion et au développement d'Internet au Canada.

D'autre part, Internet n'est pas propice aux formes traditionnelles de contrôle de contenu, tels que les règlements concernant la radiodiffusion, et ce principalement en raison de sa nature internationale et du mécanisme sous-jacent de communication par paquets. Toute tentative de réglementation, à un niveau national, de la circulation de l'information sur Internet coûterait extrêmement cher, nuirait à la performance du réseau et serait facilement contournable (il suffit d'obtenir un accès Internet dans une juridiction qui n'est pas réglementée); ce genre de réglementation est donc inapplicable, si toutefois elle est réalisable du point de vue technologique. Ce sont certaines des constatations qui ressortent du rapport commandé par Industrie Canada et qui s'intitule Réglementation d'Internet - une perspective technologique[3].

Autre point tout aussi important: la réglementation n'est pas considérée, sous l'angle de la politique gouvernementale, comme un moyen efficace de régler le problème que pose le contenu offensant sur Internet. Cette question a été abordée de façon assez détaillée lors des audiences sur les nouveaux médias tenues par le CRTC (Conseil de la radiodiffusion et des télécommunications canadiennes)[4]; le CRTC y expose son approche en ce qui concerne les services Internet, à savoir qu'il ne réglementera pas ces services en vertu de la Loi sur la radiodiffusion. Le CRTC indique également qu'il existe plusieurs méthodes basées sur le marché et la technologie, méthodes qui permettent de contrôler le contenu offensant sur Internet et qui, à son avis, vont plus dans le sens des objectifs de la politique gouvernementale que ne le ferait la réglementation.

---

[3] Gerry Miller et al. (mars 1999). *Réglementation d'Internet - une perspective technologique*. [En ligne]. DFSIonible à : //http://strategis.ic.gc.ca/SSG/it05082f.html. [janvier 2000]

[4] Présentations aux audiences sur les nouveaux médias, CRTC, 1999, dFSIonibles à [www.crtc.gc.ca].

Parmi les mécanismes proposés dans le document intitulé Réglementation d'Internet - une perspective technologique, mentionnons les technologies de filtrage au niveau du poste de travail, lesquelles permettent à l'utilisateur de filtrer le contenu auquel il peut accéder depuis son ordinateur. Au lieu d'extraire des éléments du Web, les systèmes de filtrage restreignent de façon sélective l'accès à des documents du Web. Ces systèmes peuvent être utilisés pour « éliminer » les sites ou les pages Web qui contiennent des éléments répréhensibles pour un groupe d'utilisateurs donné. Ces systèmes pourraient par exemple servir à empêcher les enfants d'accéder à des sites contenant du matériel pornographique.

Dans le cas de ce genre de filtrage, l'idée est qu'il vaut mieux laisser échapper certains documents plutôt que d'obtenir des documents offensants; autrement dit, la précision est plus importante que l'extraction comme telle. Toutefois, les mécanismes de filtrage sont difficiles à maintenir dans un environnement auquel on ajoute sans cesse de nouveaux éléments et dans lequel les nouvelles technologies Web continuent de se développer. Pour fonctionner de façon efficace, les systèmes de filtrage doivent acquérir et maintenir à long terme des connaissances précises non seulement sur les utilisateurs mais aussi sur les documents.

Bien que ces technologies ne soient pas efficaces à cent pour cent (les mordus d'informatique peuvent toujours les contourner, on ne peut pas vraiment s'y fier pour filtrer tout le contenu indésirable et certains contenus peuvent être filtrés involontairement), elles constituent tout de même une partie importante de la boîte à outils de contrôle de contenu de l'utilisateur. Dans un rapport récent intitulé Youth Access to Alcohol and Tobacco Web Marketing: The Filtering and Rating Debate[5], le Center for Media Education donne une bonne critique des filtres de contenu, rend compte de divers tests et recense en détail les technologies de sélection, de filtrage et de contrôle.

Les technologies de filtrage qui évoluent sont celles qui sont mises en œuvre au niveau du fournisseur de services Internet (FSI).[6] Voici ce qu'elles comprennent :

- Services en ligne "axés sur la famille", lesquels filtrent le contenu en limitant le domaine auquel les enfants ont accès lorsqu'ils sont en ligne.
- Filtrage manuel du contenu d'après la politique de l'FSI en ce qui concerne l'usage acceptable.
- Mécanismes de contrôle de l'accès (comme des interfaces de préinscription ou de validation de carte de crédit).
- Chiffrement et autres méthodes de codage.

---

[5] Center for Media Education. (octobre 1999). *Youth Access to Alcohol and Tobacco Web Marketing: The Filtering and Rating Debate*. [En ligne]. DFSIonible à : http://www.cme.org [janvier 2000].

[6] McRae, Philip et al. (juin 1998). *Blocking Content on the Internet: A Technical Perspective*. [En ligne]. DFSIonible à : http://www.cmis.csiro.au/projects+sectors/blocking.pdf. [janvier 2000].

Rapport produit pour le Australian National Office for the Information Economy par CSIRO Mathematical and Information Sciences (juin 1998). Ce rapport donne une description des technologies de blocage qui peuvent être utilisées par les FSI.

- Technologies de filtrage et de blocage (dont la nouvelle famille des technologies de filtrage utilisant l'antémémoire).

Ces mécanismes peuvent être très prometteurs au niveau de la gestion du contenu, surtout s'ils permettent à l'utilisateur d'avoir un certain contrôle. Ils peuvent également offrir un système technologiquement plus robuste auquel les parents pourront se fier davantage, comparativement aux filtres d'ordinateur, qui sont plus susceptibles d'être trafiqués.

Lorsqu'on élabore des stratégies de filtrage, il faut savoir qu'il existe plusieurs catégories d'intervenants, du producteur de contenu au consommateur lui-même.

- Les producteurs de contenu peuvent fournir des métadonnées autoréférentes ou des étiquettes qui décrivent le contenu de leurs pages et qui peuvent être utilisées par d'autres pour exclure ou inclure ces pages.
- Les tiers peuvent fournir aux utilisateurs un service d'évaluation fiable. Ces tiers garantissent généralement l'étiquetage des pages, soit par la lecture et l'évaluation des sites, soit par l'accumulation d'évaluations collectives de sites, évaluations qu'ils fournissent selon les besoins. Les tiers peuvent fournir, sous forme de service, des listes d'adresses Web (URL) appropriées ou inappropriées d'après l'évaluation du contenu des sites.
- Les fournisseurs de services Internet (FSI) peuvent fournir à leurs clients un service qui bloque l'accès à des sites ou qui offre une liste d'URL privilégiés. En règle générale, le FSI utilise des étiquettes d'évaluation (qu'il a créées lui-même ou qu'il a obtenues d'un tiers), des listes d'URL privilégiés ou des listes noires d'URL (qu'il a lui-même créées ou qu'il a obtenues d'un tiers), ou encore des algorithmes pour filtrer les demandes en fonction du contenu réel des requêtes ou des pages extraites.
- Les clients peuvent également effectuer des opérations de filtrage au niveau de leur ordinateur. En général, les logiciels pour ordinateurs utilisent des étiquettes d'évaluation et des listes pour accepter ou bloquer les URL ou pour bloquer les pages en examinant le contenu extrait.

Bien qu'il soit possible de mettre en œuvre certains mécanismes de filtrage au niveau de l'ordinateur client, ce sont les mécanismes que les FSI ont le *choix* d'offrir et que les utilisateurs peuvent *choisir* d'utiliser qui font l'objet de cette étude.

Nous nous pencherons d'abord, dans cette étude, sur le filtrage des pages Web, puis sur celui du courrier électronique, des sites ftp, de telnet, des groupes de discussion, des groupes de bavardage et des groupes de nouvelles, comme les listes Usenet ou les applications de messagerie instantanée. Le chapitre 2 présente un plan de classification à deux couches des technologies de filtrage. Le chapitre 3 traite de ces couches en détail. Le chapitre 4 donne une évaluation de ces technologies et de ces applications, tandis que le chapitre 5 indique à quel niveau doit se faire le filtrage. Le chapitre 6 donne une récapitulatif des technologies abordées et présente des recommandations en ce qui concerne leur utilisation.

## 2. Plan de classification des technologies de filtrage

### 2.1. Plan à deux couches

Le plan de classification qui décrit les technologies de filtrage se compose de deux couches : la couche technologies de base et la couche applications. La couche technologies de base comprend les catégories de technologies de base qui peuvent être combinées ou utilisées séparément par les applications de la couche applications. La couche technologies de base comprend les éléments suivants : étiquettes de sites, listes « blanches » et listes « noires » d'URL, analyse automatique du texte, contrôle des droits d'accès et repérage des activités. La couche applications, elle, comprend les éléments suivants : logiciels mandataires, navigateurs spécialisés, moteurs de recherche spécialisés, moniteurs d'activité et applications de contrôle d'accès.

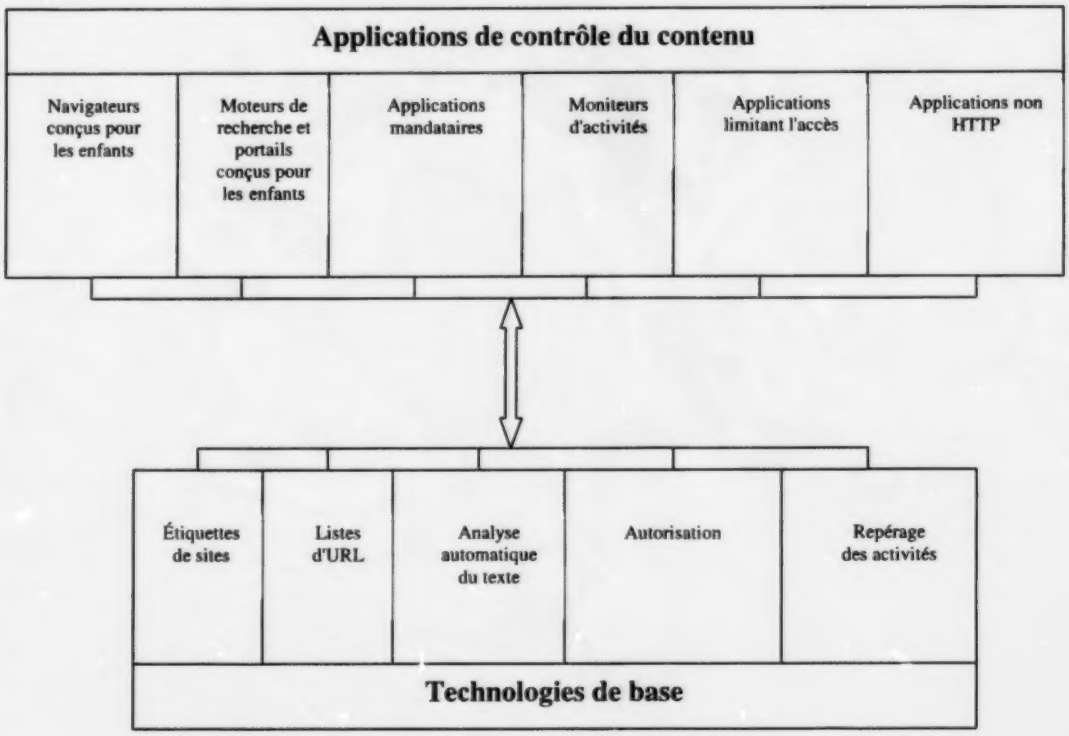


**Figure 1. Applications et technologies de base**

### 2.1.1. Technologies de base

Les catégories de technologies de base énumérées ci-dessous seront utilisées dans ce rapport pour décrire les méthodes de filtrage de contenu Internet qui sont offertes aujourd'hui.

- **Étiquetage des sites.** L'étiquetage désigne les mécanismes utilisés pour attribuer à des URL et à des pages Web précises des étiquettes liées au contenu. Les protocoles d'évaluation individuels sont généralement séparés des produits ou des applications qui les utilisent. En règle générale, les étiquettes qui sont attribuées peuvent être enregistrées dans la page Web ou séparément, dans une base de données. Ces étiquettes peuvent être attribuées selon une autoévaluation, selon l'évaluation de services indépendants ou encore selon l'évaluation de groupe d'utilisateurs concernés[7].
- **Listes de sites appropriés ou de sites inappropriés (listes « blanches » et listes « noires »).** La méthode de filtrage la plus courante consiste à utiliser des listes d'URL acceptables et/ou inacceptables. Les listes « blanches » servent à définir un domaine de sites Web « sûrs » dans les limites duquel les utilisateurs peuvent naviguer. Ce genre de liste exige normalement de rechercher et de sélectionner des sites qui sont approuvés par le fournisseur de la liste. Les listes « noires », elles, sont des listes compilées d'adresses URL pour lesquelles les demandes ne seront pas honorées. Ces listes sont compilées à titre de service par des utilisateurs individuels ou par des groupes d'évaluateurs.
- **Analyse automatique du texte.** Une autre façon d'analyser un site Web consiste à utiliser un logiciel qui analyse le texte du site pour en déterminer la pertinence ou la convenance. Les utilisateurs ou les groupes d'utilisateurs ont des profils d'intérêts (positifs et/ou négatifs) composés de mots-clés et d'expressions, qui servent justement à établir cette pertinence. Presque tout le filtrage basé sur le contenu utilise une forme de couplage de mots-clés, les mots-clés d'un profil d'intérêts étant comparés avec les mots-clés du contenu d'une page Web donnée. L'analyse du texte est également utilisée pour sélectionner des termes de recherche à partir des requêtes.
- **Autorisation.** Le chiffrement, la protection par mot de passe et la validation des cartes de crédit sont des méthodes utilisées pour certifier qu'un utilisateur a l'autorisation d'accéder à certains services ou à certaines données.
- **Repérage des activités.** L'utilisation qui est faite d'Internet peut être retracée à l'aide des fichiers journaux du serveur. Ces fichiers enregistrent les détails de tous les accès au Web.

---

[7] J.Balkin, B.Noveck, K.Roosevelt Filtering the Internet: A best practices model. In *Protecting our children on the Internet. Towards a new culture of responsibility.* J.Waltermann et M.Machill (eds). Bertelsmann Foundation Pub. 1999.

### 2.1.2. Applications de filtrage

Les mécanismes de filtrage sont mis en œuvre dans les applications logicielles susceptibles de résider dans l'hôte du FSI, du client ou d'un autre intervenant. Ces applications utilisent une ou plusieurs des technologies de base et peuvent être réparties grosso modo dans les catégories suivantes :

- **Navigateurs pour enfants.** Il est possible de créer des navigateurs à l'intention des jeunes utilisateurs. Ces navigateurs peuvent offrir des stratégies de recherche simplifiées et des graphiques plus conviviaux, supprimer les annonces publicitaires et fournir des fonctions de filtrage et des domaines de recherche sûre de façon transparente.
- **Moteurs de recherche et portails axés sur les intérêts des enfants**. L'idée est d'utiliser, dans ces deux cas, une passerelle de tiers qui donne accès au contenu du Web. Les portails conçus pour les enfants sont des sites d'accès au Web qui essaient de fournir un domaine de sites sûrs que l'utilisateur peut explorer. Du moment qu'il passe par le portail, l'utilisateur ne peut visualiser qu'un ensemble de domaines présélectionnés du Web.
- **Applications mandataires.** Les applications mandataires sont des logiciels au niveau du FSI qui font office d'intermédiaire entre le client ou le navigateur et Internet. Un logiciel d'application peut être ajouté aux modules mandataires du serveur, et ce, pour permettre l'analyse du texte et la comparaison des listes d'URL à chaque demande et réponse du navigateur Internet.
- **Moniteurs d'activité**. Plutôt que de limiter ou de contrôler l'accès aux sites Web de façon proactive, ces applications surveillent et enregistrent les activités effectuées sur Internet pour que les parents puissent les examiner ultérieurement.
- **Applications limitant l'accès aux données**. Les applications qui résident sur le site hôte peuvent être écrites de façon à ne permettre qu'aux utilisateurs autorisés d'accéder aux données ou aux services offerts sur ce site. Ces applications peuvent chiffrer les données de sorte que seuls les utilisateurs autorisés puissent les déchiffrer et les visualiser.
- **Applications autres que des applications HTTP.** Outre les applications qui limitent l'accès aux pages Web, il est possible de créer des applications à l'aide de ces technologies de base pour filtrer le contenu du courrier électronique et pour contrôler l'accès aux sites FTP, aux hôtes Telnet, aux groupes de discussion et de bavardage et aux groupes de nouvelles.

En général, les technologies de filtrage peuvent être appliquées de façon proactive ou de façon réactive. Ces mécanismes ne sont pas disjoints, mais la philosophie d'application diffère. Les FSI et les tiers fournissent des services proactifs pour évaluer le contenu des sites Web et accumuler des données sur le filtrage du contenu. Les clients et les FSI appliquent généralement des mécanismes réactifs pour utiliser ces données de filtrage afin d'autoriser ou de bloquer l'accès à du matériel offert sur le Web.

Les mécanismes de filtrage proactifs ou de prérecherche désignent les activités de prérecherche qui collectent l'information susceptible d 'être utilisée pour empêcher

l'extraction de pages inappropriées ou pour définir des domaines de sites Web appropriés à l'intention de groupes d'utilisateurs. Les mécanismes de filtrage proactifs comprennent les activités suivantes : création, stockage et utilisation d'étiquettes et création de listes de bons et de mauvais URL. Étiquettes et listes d'URL exigent de longs travaux d'identification des ressources et de repérage des sites appropriés et inappropriés.

Le filtrage réactif ou de postrecherche désigne l'analyse des noms de domaine des URL, des métadonnées ou du contenu après qu'une recherche a été exécutée sur le Web. Ces mécanismes peuvent également utiliser les listes d'URL et l'évaluation des étiquettes associées à des pages données. De plus, le filtrage de postrecherche peut utiliser une méthode basée sur le contenu pour analyser le contenu réel des pages renvoyées par la recherche et, selon les résultats, autoriser ou interdire l'accès à ces pages. Les tableaux ci-dessous résument les rôles qu'ont les intervenants - propriétaires de sites, tiers, FSI et clients - dans les activités proactives et réactives. Dans le tableau 1, nous voyons que tous les intervenants peuvent participer aux activités de repérage, allant de l'autoappréciation au repérage dynamique au moment de la recherche (ou une combinaison d'activités). Dans le tableau 2, nous voyons que les activités réactives sont en grande partie gérées par le logiciel du FSI, du client ou des deux.

| **Proactif** | **Fournisseur de contenu** | **Évaluation de tiers** | **FSI** | **Client** |
|---|---|---|---|---|
| **Étiquettes de sites** | Autoappréciation | Recherche/ création | | |
| **Listes d'URL** | | Recherche/ création | Création | Création |
| **Analyse du texte** | | Évaluation automatique | Recherche sur le Web | |
| **Navigateurs** | | | | Oui |
| **Moteurs de recherche** | | | Filtrage des requêtes et des sites | Filtrage des requêtes et des sites |

**Tableau 1. Mécanismes de filtrage proactifs**

| Réactif | Fournisseur de contenu | Évaluation de tiers | FSI | Client |
|---|---|---|---|---|
| **Étiquettes de sites** | | | Filtrage des résultats | Filtrage des résultats |
| **Listes d'URL** | | | Filtrage des résultats | Filtrage des résultats |
| **Analyse du texte** | | | Filtrage des résultats | Filtrage des résultats |
| **Navigateurs** | | | | Filtrage des résultats |
| **Moteurs de recherche** | | | Filtrage des résultats | |

**Table 2. Mécanismes de filtrage réactifs**

## 2.2. Modes d'accès

Les données sont, sur Internet, disponibles dans de nombreux modes d'accès, au moyen du protocole Web originel, HTTP (Hypertext Transport Protocol), et de protocoles autres que HTTP, dont : le courrier électronique, ftp, telnet, les forums, les groupes de discussion, les serveurs de nouvelles, les babillards électroniques et les services de messagerie instantanée.

*Navigateurs.* Les navigateurs, tels Netscape et Internet Explorer, sont généralement utilisés pour accéder aux pages Web, indiquées par des URL, à l'aide du protocole HTTP. Les catégories de contrôle d'accès mentionnées précédemment s'appliquent toutes à l'accès HTTP. Le protocole HTTP standard exige un en-tête HTTP décrivant la demande ou la réponse, ainsi qu'un fichier document.

*Courrier électronique* - le courrier électronique peut être utilisé par des applications de courrier autonomes ou comme application du navigateur. Le courrier électronique utilise divers protocoles, habituellement le protocole POP (Post Office Protocol) ou SMTP (Simple Mail Transfer Protocol). La plupart des applications de courrier électronique permettent de joindre des fichiers au message. Les restrictions d'accès au courrier électronique suivent deux grands principes : filtrage des messages entrants à partir des sources désignées ou par sujet limité, et filtrage par analyse du contenu réel du message. Les fichiers joints, qui peuvent être des images ou des vidéos, sont très difficiles à filtrer de façon efficace.

*Serveurs de nouvelles* - le protocole NNTP (Network News Transport Protocol) gère les serveurs de groupes de nouvelles, comme le très répandu Usenet, qui fonctionne depuis 1979. Usenet est un système d'échange du style babillard électronique qui fait appel au protocole NNTP pour permettre à n'importe quel utilisateur de poster des messages sur un des milliers de sujets classés sous forme de hiérarchie. Les serveurs NNTP mettent ensuite ces messages à la dFSIosition des membres du groupe de nouvelles. Des fichiers de nouvelles sont constamment envoyés aux serveurs de nouvelles, ce qui permet de filtrer le contenu par fichier. De plus, les groupes de nouvelles qui sont introduits dans le serveur et les utilisateurs de groupes de nouvelles qui y ont accès peuvent faire l'objet de restrictions.

*Transferts de fichier* - le protocole FTP (File Transport Protocol) est un protocole TCP/IP qui permet aux utilisateurs d'Internet de transférer facilement des fichiers d'un ordinateur à un autre. TCP/IP (Transmission Control Protocol/Internet Protocol) est l'ensemble de protocoles utilisé pour communiquer par Internet, protocoles qui garantissent que les messages sont acheminés correctement et qu'ils arriveront intacts. Le demandeur ne jouit pas nécessairement de privilèges utilisateur sur le site hôte. Le site hôte, appelé serveur FTP, peut autoriser un accès général ou anonyme aux fichiers ou restreindre l'accès à ses fichiers, un id-utilisateur et un mot de passe étant alors exigés. La plupart des navigateurs ouvriront également une session FTP pour les URL commençant par « ftp:// ».

*Telnet* - Telnet est un autre protocole TCP/IP qui permet à l'utilisateur d'un ordinateur de se connecter à un compte d'un autre ordinateur. Contrairement à HTTP ou à FTP, le protocole Telnet offre un accès complet aux applications et aux données de l'ordinateur hôte.

Il est relativement difficile de contrôler les accès FTP et Telnet, car les applications sont exécutées en dehors des navigateurs classiques. Des listes de contrôle d'accès à des hôtes acceptables ou inacceptables peuvent être utilisées. Comme il se peut qu'une grande partie des données ne soient pas en clair, le filtrage du contenu est problématique.

*Groupes de discussion* - les groupes de discussion sont des variantes HTTP des groupes de nouvelles; ici, le nombre de membres est souvent réduit et le sujet très précis. Par exemple, un groupe de travail ou une catégorie d'utilisateurs pourrait créer son propre site

de groupe de discussion. Un groupe de discussion permet à ses membres de communiquer de façon asynchrone, c'est-à-dire qu'il leur permet de poster des questions ou des commentaires, tandis que d'autres membres postent leurs réponses ou leurs opinions de façon hiérarchique.

*Groupe de bavardage* - le groupe de bavardage est une variante synchrone ou en temps réel du groupe de discussion; ici, les commentaires sont échangés en temps réel sur un sujet intéressant les membres actifs du groupe. En règle générale, les utilisateurs qui se trouvent « dans » le salon de bavardage peuvent voir tous les messages. Les échanges peuvent être enregistrés, mais il se peut aussi qu'ils ne puissent l'être.

*Messagerie instantanée* - ICQ est la plus importante des applications de messagerie instantanée qui existe actuellement. Les applications ICQ et du type ICQ font office de groupe de bavardage, car elles permettent d'échanger des messages en temps réel, mais elles indiquent également aux membres qui d'autre est en ligne.

La question du contrôle d'accès aux groupes de discussion, aux groupes de bavardage et à ICQ se situe au niveau de la pertinence des membres du groupe particulier. Les parents peuvent alors choisir d'interdire tout accès à ces applications ou de définir un accès approprié.

## 3. Description des technologies de filtrage

Dans ce chapitre, nous décrirons les technologies sous-jacentes qui sont utilisées dans les divers mécanismes de filtrage. Les technologies de base sont traitées dans la section 3.1 et les catégories d'application dans la section 3.2.

Nous n'analyserons pas, dans ce rapport, la portée des préoccupations sociales et politiques, laquelle est cruciale pour la mise en place adéquate de toute politique. Le succès de ces technologies repose sur le lien entre les valeurs collectives et l'élaboration de politiques qui peuvent être mises en œuvre par la technologie. La technologie doit être utilisée pour mettre en œuvre les valeurs collectives, non pour les dicter.

### 3.1 Technologies de base

#### 3.1.1 Systèmes d'étiquetage de sites

L'étiquetage désigne les mécanismes utilisés pour attribuer à des URL et à des pages Web précises des étiquettes liées au contenu. Les protocoles d'évaluation individuels sont généralement séparés des produits ou des applications qui les utilisent. En règle générale, les étiquettes qui sont attribuées peuvent être enregistrées dans la page Web ou séparément, dans une base de données. Ces étiquettes peuvent être attribuées selon une autoévaluation, selon l'évaluation de services indépendants ou encore selon l'évaluation de groupes d'utilisateurs concernés[8]. L'autoévaluation désigne l'acte par lequel les concepteurs de pages Web fournissent une étiquette décrivant le contenu de leurs pages. La qualité de ces étiquettes reflète l'intérêt personnel du concepteur. L'évaluation de services indépendants ou tiers indique que ce sont des groupes ou des entreprises qui se chargent de fournir, à l'intention de leurs clients ou de leur groupe d'utilisateurs, des étiquettes décrivant le contenu des pages Web. Les évaluations collectives sont les plus officieuses, car elles sont faites par des internautes animés des mêmes idées, qui partagent mutuellement ce qu'ils savent du contenu des pages Web.

L'utilisation d'étiquettes pour filtrer le contenu nécessite plusieurs opérations : création, stockage, mise à jour et diffusion des étiquettes, authentification des donnés des étiquettes et enfin utilisation de ces données par les logiciels de filtrage pour classifier les pages Web dans la catégorie acceptable ou la catégorie inacceptable pour le contexte visé.

##### 3.1.1.1 Création d'étiquettes de sites

*Protocoles d'étiquetage*

[8] Idem p. 10.

Bien qu'il existe divers protocoles ou systèmes d'étiquetage, il n'y en a que quelques-uns qui soient répandus sur Internet.

Le Recreational Software Advisory Council, qui fait maintenant partie de la Internet Content Rating Association[9] (ICRA), utilise un système d'autoévaluation volontaire, soit le système de classification RSACi[10]. Le système RSACi évalue les sites d'après quatre catégories (langage, nudité, sexe et violence) et donne aux utilisateurs des informations sur les niveaux (de 0 à 4) de ces catégories dans des sites donnés. RSACi est maintenant utilisé par Internet Explorer, CyberPatrol et CompuServe (aux États-Unis et en Europe).

SafeSurf[11] est un système d'évaluation à onze catégories (tranche d'âge, blasphèmes, thèmes hétérosexuels, thèmes homosexuels, nudité, violence [sexe, violence et blasphèmes], intolérance, préconisation de l'usage de drogues, autres thèmes adultes, jeux de hasard). Dans les deux systèmes, chaque grande catégorie est divisée en plusieurs sous-catégories. SafeSurf est utilisé par Netscape Navigator et Internet Explorer[12].

Adequate.com[13] est un système d'évaluation basé sur les systèmes américains de classement des émissions de télévision. Les sites destinés aux enfants sont classifiés pour tous les enfants ou pour les enfants plus âgés. Les autres sites peuvent être classifiés comme suit : général, surveillance parentale, forte mise en garde des parents ou adulte seulement.

Le Entertainment Software Rating Board (ESRBi)[14] possède un système d'évaluation des sites Web qui offrent des jeux. Les catégories de ce système sont les suivantes : petite enfance, enfants à adultes (catégorie intitulée maintenant pour tous), adolescents, adultes, adultes seulement. Chacune de ces catégories peut être élargie pour comprendre des descripteurs de contenu, notamment le degré et le type de violence, le langage (décent ou grossier), le genre de contenu sexuel et la pertinence pour de jeunes enfants.

Le Dublin Core[15] est le système le plus connu pour identifier les documents Web de façon descriptive. Ce système comprend un jeu de descripteurs prédéfinis qui sont utilisés pour étiqueter le contenu des pages. Les descripteurs actuels sont les suivants : titre, auteur, sujet, description, éditeur, collaborateur, date, type, format, identificateur, source, langue, relation, couverture, droits.

---

[9] *ICRA Internet Content Rating Association.* 2000 [En ligne]. DFSIonible à : http:// www.icra.org [janvier 2000]

[10] *RSAC Recreational Software Advisory Council.* 2000. [En ligne]. DFSIonible à : http://www.icra.org. [janvier 2000]

[11] *SafeSurf* [En ligne]. DFSIonible à : http://www.safesurf.com. [janvier 2000]

[12] Center for Media Education. (October 1999). *Youth Access to Alcohol and Tobacco Web Marketing: The Filtering and Rating Debate.* [En ligne]. DFSIonible à : http://www.cme.org [janvier 2000]

[13] *Adequate* [En ligne]. DFSIonible à : http://www.adequate.com [janvier 2000].

[14] *ESRB Entertainment Software Rating Board.* 1999. [En ligne]. DFSIonible à : http://www.esrb.org [janvier 2000].

[15] *Dublin Core Metadata Initiative.* 2000. [En ligne]. DFSIonible à : http://purl.org/dc [janvier 2000]

*Langages de mise en œuvre des étiquettes*

Une fois qu'un système d'étiquetage a été choisi par un service ou un groupe, on a besoin d'un langage, comme le langage PICS (Platform for Internet Content Selection[16]) ou des métadonnées HTML, pour pouvoir l'appliquer à des pages Web individuelles. HTML (Hypertext Markup Language) est l'ensemble de balises et de règles utilisées pour marquer les documents Web qui seront interprétés par le navigateur avant d'être affichés. XML peut souvent être utilisé pour définir ces langages à utiliser sur Internet, comme l'indique la figure ci-dessous. XML (Extensible Markup Language) est un langage permettant de créer des langages de balisage.

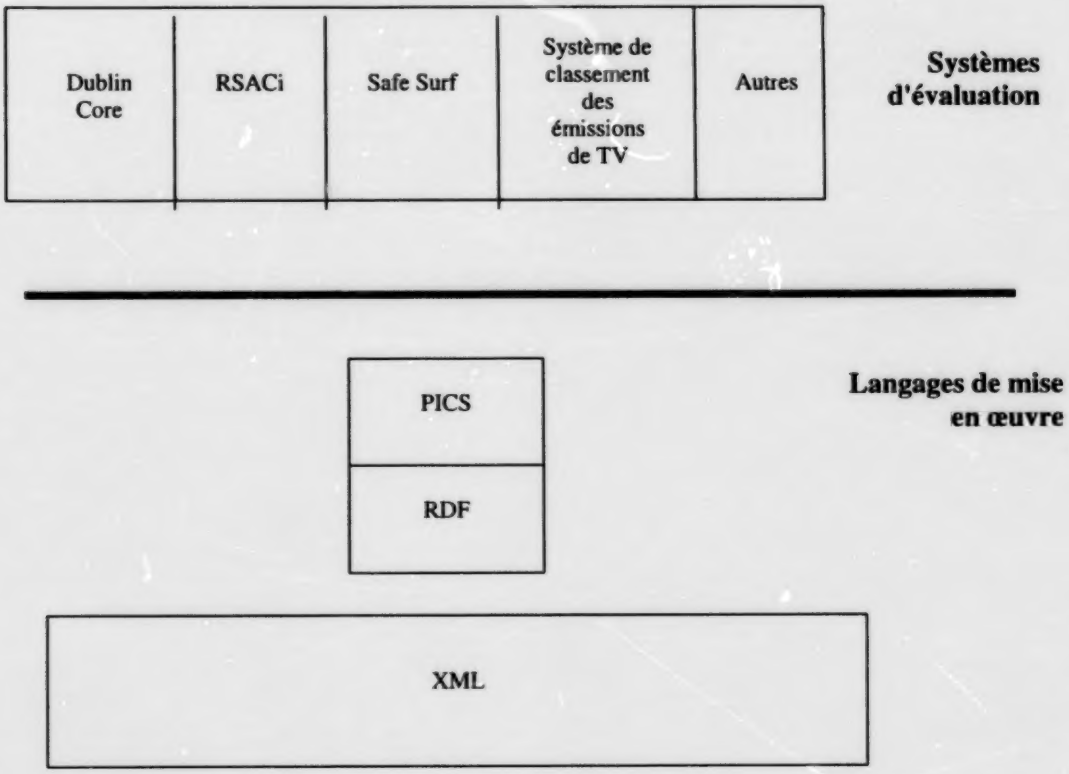


**Figure 2. Protocoles d'étiquetage et langages de mise en œuvre**

Le protocole PICS pour les étiquettes associées à du contenu Internet a été mis au point en 1995 et continue d'être amélioré par le Consortium du World Wide Web (CW3). La plate-forme PICS est une plate-forme sur laquelle d'autres services d'évaluation et d'autres logiciels de filtrage ont été créés. Elle est utilisée par les logiciels pour étiqueter

[16] *Platform for Internet Content Selection (PICS)*. 1999. [En ligne]. DFSIonible à : http://www.w3c.org/PICS [janvier 2000]

le contenu des pages à des fins particulières, comme déterminer si certaines pages Web conviennent aux enfants qui naviguent sur Internet. PICS n'est pas un logiciel de filtrage, mais peut être utilisé par des services de filtrage ou d'évaluation pour créer des catégories communes d'étiquettes. PICS est un ensemble de règles qui peuvent servir à définir des étiquettes décrivant le contenu de pages Web et pouvant être partagées par un groupe d'utilisateurs. Les logiciels partagés peuvent alors utiliser les règles PICS pour interpréter les données d'étiquetage à des fins de filtrage.

Voici un exemple de liste d'étiquettes PICS, qui a été lui-même adapté d'un exemple du W3C. Ici, le bureau d'étiquettes (base de données d'étiquettes distincte) se trouve à l'adresse http//www.abc.org/r1.5. De plus, une étiquette pour le site *http:www.xyz.com/new.html* a été créée par John Doe et est valide du 5 novembre 1998 au 1er novembre 2000; l'évaluation de ce site est faible (bonne) en ce qui concerne la violence et le sang, mais est élevée (médiocre) en ce qui concerne le langage.

```
(PICS1-1 "http//www.abc.org/r1.5"
        by "John Doe"
        labels on "1998.11.05"
              until "2000.11.01"
        for http://www.xyz.com/new.html
        ratings (violence 2  blood 1  language 4))
```

Le Consortium du World Wide Web a également mis au point deux éléments d'amélioration pour les applications qui utilisent les protocoles PICS. Le premier, appelé PICSRules[17], permet à une application compatible avec PICS de télécharger des règles de tiers qu'elle peut utiliser pour traiter les données PICS afin de contrôler l'accès au contenu du Web à ce site. Dans l'exemple suivant, le PICSRule de blocage utilise l'URL pour bloquer l'accès à toute page Web du domaine http://www.xyz.com.

```
(PicsRule-1.1
        (Policy (RejectByURL (http://www.xyz.com:*/*)
         Policy (AcceptIf "otherwise")))
```

Voici maintenant un exemple de PICSRule de blocage qui pourrait être utilisé par une application. Les données d'étiquetage seraient téléchargées à partir d'un bureau d'étiquettes de tiers.

```
(PicsRule-1.1
        (serviceinfo (
                http://www.lablist.org/ratings/v1.html
                shortname "PTA"
                bureauURL http://www.lablist.org/ratings
                UseEmbedded "N")
```

[17] *PicsRules1.1 W3C Recommendation 29 Dec 1997.* 1999. [En ligne]. DFSIonible à : http://www.w3c.org/TR/PR-PICSRules.htm [janvier 2000]

Policy (RejectIf "((PTA.violence >3) or (PTA.language >2))")
Policy (AcceptIf "otherwise")))

Dans cet exemple, les étiquettes intégrées aux documents ne sont pas prises en compte et seules les étiquettes extraites du bureau d'étiquettes (http://www.lablist.org/ratings) à l'aide du système de classement « v1.html » sont utilisées pour évaluer les documents.

Le deuxième élément d'amélioration de PICS, qui s'intitule Dsig[18], permet aux applications compatibles avec PICS de vérifier l'authenticité des étiquettes PICS. Autrement dit, cela permet de vérifier la véracité des données relatives à une ressource, c.-à-d. de l'étiquette.

Les deux systèmes d'évaluation PICS qui sont utilisés à grande échelle sont ceux qui ont été mis au point par le Recreational Software Advisory Council (RSACi)[19] et par Safe Surf[20], tels que décrits précédemment.

Le RDF (Resource Description Framework[21]), qui a été créé par le Consortium du World Wide Web, permet de créer des descriptions de ressources, de texte, de graphiques, de vidéo, etc., descriptions qui sont compréhensibles par la machine. Le RDF utilise le langage XML (e-Xtended Markup Language ) pour baliser le contenu, l'auteur, le public cible, etc. des sites Web. Le RDF offre une méthode uniforme pour fournir des métadonnées avec les documents Web. Ces données peuvent être utilisées pour déterminer quelles sont les ressources disponibles, pour évaluer du contenu et pour classifier des documents. Les utilisateurs et les groupes d'utilisateurs peuvent élaborer, à l'aide de PICS, un système partagé qui réponde à leurs besoins. Les applications RDF peuvent alors utiliser les métadonnées pour filtrer du contenu. Les descripteurs du Dublin Core sont souvent utilisés avec RDF.

Voici un exemple de descripteur de document RDF :

```
<RDF>
<Description about-"http://cs.dal.ca/index.html">
<DC:title>page de la faculté de CS</DC:title>
<DC:creator>J. Dupont</DC:creator>
<DC:date>2000-01-03</DC:date>
<DC:subject>cours universitaires</DC:subject>
<DC:audience>étudiants de niveau universitaire</DC:audience>
</Description>
</RDF>
```

---

[18] *DSig 1.0 Signature Label Specification: W3C Proposed Recommendation 03-April-1998.* 1999. [En ligne] DFSIonible à : http://www.w3c.org/TR/REC-Dsig-label/ [janvier 2000].
[19] *RSACi Recreational Sofware Advisory Council.* 2000. [En ligne]. DFSIonible à : http://www.icra.org [janvier 2000]
[20] *SafeSurf.* [En ligne]. DFSIonible à : http://www.safesurf.com [janvier 2000]
[21] *Resource Description Framework (RDF).* 1999. [En ligne]. DFSIonible à : http://www.w3.org//RDF [janvier 2000]

Des logiciels[22] peuvent être créés pour générer automatiquement des métadonnées en format RTF, métadonnées qui décrivent des documents HTML. Ces métadonnées RTF peuvent être ensuite utilisées dans le processus de filtrage.

Des métabalises HTML peuvent être insérées dans des pages Web. Un document Web est normalement constitué de texte balisé en HTML, où les caractéristiques d'affichage de la page sont définies par des balises, comme <P> ou <B>. Un document HTML peut avoir à la fois un en-tête, défini entre les balises <HEAD>...</HEAD> et un corps, défini entre les balises <BODY>....</BODY>. Les métabalises peuvent être utilisées, dans l'en-tête d'un document HTML, pour décrire le contenu du document, sa qualité, etc., et ce, à l'intention du navigateur ou du serveur (ou des deux). Les données de ces balises n'apparaissent pas dans le navigateur, mais ce dernier peut les utiliser pour afficher la page. Les logiciels de serveur peuvent également utiliser les valeurs de ces champs comme des éléments de champs d'en-tête HTTP, et ce, pour répondre aux demandes visant ce document.

Chaque métabalise (<META>) comprend deux parties, HTTP-EQUIV et NAME, lesquelles sont utilisées pour définir une paire nom-valeur, comme "keyword=enfant". Il est possible de créer une concaténation de plusieurs métabalises pour former une liste.

Par exemple, un document HTML pourrait comporter les balises de métadonnées suivantes dans son en-tête ( HEAD) :

```
<HEAD>
        <META HTTP-EQUIV="keywords" CONTENT="nudité">
        <META HTTP-EQUIV="keywords" CONTENT="sexe' >
</HEAD>
```

Lorsque ce document est demandé, le serveur inclut les métadonnées dans l'en-tête de réponse HTTP et le logiciel client peut alors utiliser ces données pour autoriser ou interdire l'accès à cette page.

*Attribution d'étiquettes*

Une fois qu'un système d'évaluation a été choisi, la prochaine étape du processus est l'attribution d'étiquettes de contenu aux pages ou aux sites Web. Ceci est le lien le plus faible du processus, car les étiquettes peuvent être attribuées à divers niveaux, avec des résultats fort différents :

- Les auteurs peuvent évaluer eux-mêmes leurs pages ou leur site et fournir des étiquettes à l'intention des lecteurs de ces pages.

---

[22] Jenkins, C., et al.. Automatic RDF metadata generation for resource discovery. *In Proceedings of WWW8 Conference*. Toronto, 11 au 14 mai 1999. Elsivor Science. 227-42.

- Un groupe d'évaluateurs peut examiner et évaluer les pages indépendamment des auteurs et fournir, à titre de service, des étiquettes aux utilisateurs.
- Certains groupes d'utilisateurs peuvent évaluer individuellement des pages et partager les données des étiquettes.
- Certains logiciels utilisent des programmes d'analyse de texte qui analysent le contenu des pages et attribuent des étiquettes d'évaluation selon des mots-clés.

#### 3.1.1.2 Gestion des étiquettes de sites

Une fois générées et attribuées, les étiquettes de sites doivent être enregistrées de façon à être accessibles. Ces métadonnées peuvent être stockées dans une base de données séparée accessible par le biais des requêtes, encapsulées dans un format spécial reconnu par l'application Web, tel le format RDF (Resource Description Framework), ou faire simplement partie de la page Web (à titre de métabalise).

*Enregistrement des données des étiquettes*

Une fois générées, les étiquettes doivent être enregistrées de façon à ce que le logiciel du FSI ou du client puisse les utiliser pour exécuter des opérations de filtrage. En règle générale, les étiquettes peuvent être intégrées à la page Web par le biais de métabalises, être associées à la page par le biais d'un système comme RDF ou être enregistrées séparément dans une base de données d'étiquettes, parfois appelée bureau d'étiquettes (Label Bureau).

Si les étiquettes sont intégrées au document Web, l'enregistrement et la récupération des données sont alors très simples. Les données sont enregistrées avec le document et envoyées en même temps que celui-ci. Normalement, les étiquettes autodescriptives sont enregistrées avec le document. Si elles sont générées indépendamment de la création du document Web, les données des étiquettes peuvent être alors enregistrées sur le même site ou même n'importe où. Le bureau d'étiquettes se charge alors de l'authentification pour ceux qui utilisent ses étiquettes.

Le contrôle des étiquettes et de leur extraction s'effectue des façons suivantes :

- Les étiquettes sont intégrées au document HTML par le producteur du document.
- Chaque FSI tient à jour une base de données d'étiquettes à titre de service offert à ses clients.
- Un tiers fournit des étiquettes à titre de service au FSI ou à ses clients.
- Les utilisateurs individuels peuvent créer et mettre à jour des fichiers d'étiquettes personnels; ces fichiers résident alors dans l'ordinateur client et sont utilisés selon les besoins.

- Des groupes d'utilisateurs peuvent collaborer et fournir des informations pour les bases de données communes tenues à jour à titre de service par une organisation, un FSI ou un tiers.

*Distribution des données des étiquettes*

Le prochain aspect à considérer est la façon de distribuer les étiquettes afin qu'elles puissent être utilisées pour le filtrage à mesure que les pages sont sollicitées.

- Les étiquettes peuvent être intégrées aux pages Web à titre de métabalises HTML. Dans ce cas, elles sont offertes chaque fois qu'une page fait l'objet d'un accès. Dans l'exemple précédent, le logiciel client peut facilement comparer les mots-clés de métadonnées et exclure tout document contenant le mot-clé « nudité ». Certains navigateurs, comme Internet Explorer (IE), recherchent dans le document racine des étiquettes génériques pour les documents sans étiquettes spécifiques. Par exemple, une page dont l'URL est …../kidstuff/x1.html pourrait ne pas contenir ses propres métabalises; dans ce cas, ce sont les métabalises de l'URL parent…../kidstuff/ qui seraient utilisées. Ces étiquettes peuvent être envoyées par le serveur en même temps que la page Web dans l'en-tête de réponse HTTP.
- Lorsqu'elles sont enregistrées en dehors de la page Web, les étiquettes peuvent être utilisées de façon indépendante. La demande d'un URL lance une interrogation de la base de données au « bureau d'étiquettes » approprié (local, FSI ou tiers). Un bureau d'étiquettes est un serveur HTTP qui peut mémoriser ses propres étiquettes ou extraire les étiquettes d'autres sites selon les besoins. L'extraction des étiquettes et celle des pages Web sont deux transactions distinctes.
- De la même façon, les étiquettes peuvent être enregistrées sous forme de fichiers RDF, lesquels doivent également être traités dans une transaction distincte. Les fichiers RDF sont des descriptions de ressources Web individuelles, descriptions qui sont lisibles par machine. Les fichiers RDF utilisent normalement XML pour coder la description selon le système d'étiquetage, comme le Dublin Core décrit précédemment.
- Les étiquettes peuvent être envoyées par tout protocole qui utilise des en-têtes US-ASCII définis dans le protocole de courrier RFC-822, tel l'en-tête « subject ». Sont également compris le courrier électronique Internet, HTTP, et les nouvelles USENET.
- Une extension du protocole HTTP[23] permet à un client HTTP de demander qu'une ou plusieurs étiquettes figurent dans l'en-tête et soient envoyées en même temps que le document demandé. Le client peut, à l'aide du protocole HTTP, ne demander que l'en-tête (au lieu de l'en-tête et du document), de

[23] *PICS Label Distribution Label Syntax and Communication Protocols: Version 1.1 W3C Recommendation 31-October-96. W3C Consortium.* 1999. [En ligne]. Disponible à : http://www.w3c.org/TR/REC-PICS-labels [janvier 2000]

façon à pouvoir examiner les données de l'étiquette avant d'extraire le document complet.

#### 3.1.1.3 Utilisation des étiquettes de sites pour le filtrage

Pour finir, les mécanismes de filtrage utilisent les données des étiquettes pour filtrer l'accès à des pages Web individuelles :

- Lorsque la page HTML contient des métabalises, le serveur du FSI ou du client peut comparer les étiquettes de contenu figurant dans la page aux profils d'intérêts.
- Le serveur HTTP peut inclure un en-tête d'étiquette dans la réponse. Certains de ces serveurs autorisent l'ajout d'un en-tête supplémentaire à la chaîne d'en-tête HTTP, que le navigateur du client peut extraire avant de traiter le contenu des données. Dans ce cas, l'application du client peut refuser le contenu des données.
- Les étiquettes enregistrées dans des fichiers RDF peuvent être traitées par le navigateur du FSI ou du client.
- Les logiciels du client peuvent utiliser des fichiers d'étiquettes locaux pour bloquer certaines demandes URL ou interdire l'accès aux réponses. Les étiquettes peuvent être créées et enregistrées sur les ordinateurs des clients, étiquettes qui seront utilisées par le logiciel de filtrage local.
- Les serveurs mandataires peuvent filtrer les demandes et les réponses à l'aide des règles PICS.
- Les bureaux d'étiquettes situés au niveau du FSI peuvent distribuer des étiquettes PICS pour les documents se trouvant dans ce serveur. Le logiciel de filtrage du FSI peut alors rechercher dans les bureaux d'étiquettes les étiquettes qui sont pertinentes. Lorsque le client demande un URL particulier, le logiciel extrait le document en même temps qu'il recherche les étiquettes correspondantes dans la base de données du bureau d'étiquettes. Le document sera alors bloqué ou envoyé, suivant la valeur des étiquettes qui lui ont été attribuées.
- Les clients ou les FSI peuvent s'abonner à un service d'évaluation qui fournit des étiquettes sur demande.
- Un tiers peut gérer des étiquettes pour les utilisateurs. Par exemple, Adequate.com offre un système dans lequel les concepteurs Web peuvent évaluer eux-mêmes le contenu de leurs pages et obtenir un « tampon » graphique à intégrer dans la page Web. Adequate.com offre en même temps un bureau d'étiquettes central consultable.

#### 3.1.1.4 Exemples d'applications qui utilisent des étiquettes de sites

Le logiciel de filtrage lit la ou les étiquettes associées à un URL et autorise ou interdit l'accès au site d'après le système d'évaluation qui est utilisé. Le logiciel de sélection

détermine la façon d'utiliser les étiquettes, normalement selon les préférences réelles ou présumées de l'utilisateur ou du groupe d'utilisateurs.

L'utilisation de la structure PICS pour intégrer des données d'évaluation à partir de divers systèmes d'évaluation est de plus en plus acceptée. Actuellement, les deux principaux navigateurs, Netscape et Explorer, ainsi que certains services autonomes comme CyberPatrol[24] et Adequate.com, gèrent les éléments PICS.

### 3.1.2 Listes d'URL

La technologie de filtrage la plus utilisée est celle qui fait appel à des listes d'URL acceptables et/ou inacceptables. Les listes « blanches » servent à définir un domaine de sites Web « sûrs », dans les limites duquel les utilisateurs peuvent naviguer. Ce genre de liste exige normalement de rechercher et de sélectionner des sites qui sont approuvés par le fournisseur de la liste. Les listes « noires », elles, sont des listes compilées d'adresses URL pour lesquelles les demandes ne seront pas honorées. Dans la plupart des cas, ces listes sont compilées par des utilisateurs travaillant seuls ou par des groupes d'évaluateurs.

#### 3.1.2.1 Création de listes d'URL

Il y a plusieurs façons de compiler des listes d'URL :

- Les utilisateurs individuels peuvent préparer une liste locale destinée à leur propre usage.
- Des groupes d'utilisateurs, des écoles, des parents concernés, etc. peuvent contribuer à enrichir une base commune d'URL acceptables ou inacceptables.
- Les FSI peuvent dresser des listes selon les préférences présumées des clients, listes que les clients peuvent décider d'utiliser pour filtrer le contenu de sites clients individuels.
- Des tiers peuvent dresser des listes à l'intention de groupes d'utilisateurs, de façon volontaire ou dans le cadre de leurs opérations.
- Les robots Web sont des programmes qui fonctionnent de façon autonome. Avec un URL de départ, ces robots recherchent le document cible, le traitent et suivent tous les liens qui y sont intégrés. Ces programmes peuvent faire office d'agents d'évaluation qui classent les sites de façon proactive d'après des algorithmes d'analyse de contenu, bien que cette fonction ne se soit pas encore avérée très précise.

---

[24] *Cyber Patrol*. 1999. [En ligne]. DFSIonible à : http://www.cyberpatrol.com [janvier 2000]

#### 3.1.2.2 Gestion des listes d'URL

Les liste d'URL peuvent être stockées sur le site du FSI, sur l'ordinateur du client ou encore sur un site de confiance d'un tiers pour être utilisées selon les besoins. Le maintien de listes à jour a un impact direct sur l'utilité de celles-ci.

Il y a certains avantages au fait que les listes soient gérées par le FSI. Premièrement, le FSI peut utiliser une application particulière, soit une application mandataire, par l'intermédiaire de laquelle toutes les demandes des clients faites sur Internet sont traitées. Deuxièmement, les mises à jour au niveau du FSI sont partagées par tous les clients. Troisièmement, les FSI peuvent tenir plusieurs listes : des listes d'URL de niveau général, qui peuvent par exemple convenir aux enfants de moins de 10 ans, des listes collectives auxquelles peuvent participer les utilisateurs et des listes de profils personnalisées à l'intention de clients particuliers.

#### 3.1.2.3 Utilisation des listes d'URL pour les opérations de filtrage

Une fois les listes établies, leur utilisation pour le filtrage est très simple. Le logiciel de mandataire du FSI, le logiciel portail et le logiciel du client peuvent tous vérifier par rapport à la liste chaque URL demandé et chaque URL renvoyé, et ce, pour chaque requête. Le logiciel mandataire est hébergé par le FSI et fait office d'intermédiaire entre le client (ou navigateur) et Internet. Le logiciel portail réside également sur le site du serveur et offre un accès prédéfini à certains sites Internet. Les applications du client, elles, sont des applications, tel le navigateur, qui résident sur le poste de travail client et qui agissent au nom du client.

Un serveur mandataire est une application serveur qui fonctionne avec le logiciel du serveur et qui fait office de canal pour les demandes des clients. Le navigateur du client doit être configuré de façon à pouvoir utiliser le serveur mandataire. Ce serveur agit comme intermédiaire dans le processus d'accès aux pages Web. Toutes les demandes des clients passent par ce serveur mandataire et le contenu extrait d'Internet passe également par lui avant d'être envoyé à l'utilisateur. En règle générale, le serveur mandataire met en antémémoire ou enregistre sur le site du FSI les pages Web extraites. Les données mises en antémémoire permettent ainsi de réduire le temps de transmission et de téléchargement ainsi que la congestion et peuvent être utilisées pour filtrer les données avant qu'elles ne soient envoyées à l'utilisateur.

#### 3.1.2.4 Exemples d'applications qui utilisent des listes

**SurfWatch**[25] – bloque 100 000 sites jugés inappropriés, ainsi que les adresses IP et les domaines virtuels connexes - ce qui représente environ deux millions de pages.

---

[25] *SurfWatch*. 1999. [En ligne]. DFSIonible à : http://www.surfwatch.com [janvier 2000]

L'appariement de formes permet également de bloquer l'accès à des millions d'autres pages.

**CyberPatrol**[26] – utilise à la fois des listes blanches et des listes noires. La liste CyberYES répertorie 3 000 sites choisis à l'intention des enfants pour leur caractère divertissant ou éducatif. La listeCyberNOT répertorie plus de 35 000 sites dans 12 catégories jugées inappropriées aux enfants. Les enfants ne peuvent accéder à ces sites si CyberPatrol est installé. De plus, CyberPatrol lit les étiquettes PICS et peut, si l'utilisateur le choisit, faire en sorte que le filtrage ne soit effectué qu'au moyen des étiquettes PICS.

**CyberSitter** [27]– tient à jour des listes de catégories de listes « noires » qui sont téléchargées sur l'ordinateur du client. CyberSitter filtre le contenu jugé pour adulte par tous les systèmes d'évaluation PICS. Ce logiciel utilise une gamme de technologies de base ainsi que l'évaluation humaine, notamment l'analyse de texte, pour presque tout le blocage.

### 3.1.3 Analyse automatique du texte

Une autre façon d'appliquer un filtre à des pages Web consiste à utiliser un logiciel qui examine le contenu réel des pages Web, tel qu'il est représenté par les mots-clés figurant dans le texte. Les utilisateurs ou les groupes d'utilisateurs ont des profils d'intérêts (positifs et/ou négatifs), composés de mots-clés et d'expressions, qui sont utilisés pour établir la pertinence des pages analysées. Presque tout le filtrage basé sur le contenu utilise une forme de couplage de mots-clés, les mots-clés d'un profil d'intérêts étant comparés avec les mots-clés du contenu d'une page Web donnée.

L'accès au Web par le biais d'un navigateur peut être qualifié de recherche ou d'exploration. S'il effectue une recherche, l'utilisateur soumet une requête à un moteur de recherche, qui extrait l'information à partir de pages Web précédemment indexées. L'extraction est normalement basée sur le modèle booléen ou sur le modèle d'espace vectoriel[28]. Ces deux modèles ont besoin, pour la recherche, de gros fichiers à recoupement[29]. S'il se livre à de l'exploration, l'utilisateur clique sur un lien d'une page Web qui a été précédemment extraite, soit par une opération de recherche, soit par une simple exploration. La page Web désignée par le lien doit être filtrée « à la volée ». Ce

---

[26] *Cyber Patrol*. 1999. [En ligne]. DFSIonible à : http://www.cyberpatrol.com [janvier 2000]

[27] *CYBERsitter*. 1999. [En ligne]. DFSIonible à : http://www.cybersitter.com [janvier 2000]

[28] Baeza-Yates, Ricardo et Berthier Ribeiro-Neto. 1999. *Modern Information Retrieval*. Harlow, England: Addison-Wesley.

[29] Un fichier à recoupement est un index de chaque terme contenant l'emplacement de chaque occurrence de ce terme dans la base de données.

genre de filtrage s'effectue au moyen d'algorithmes de recherche sérielle par chaînes de caractères[30] et aucun fichier à recoupement n'est conservé.

Le modèle booléen fait appel aux opérateurs booléens AND, OR et NOT. La requête se compose de mots-clés joints par ces opérateurs. Par exemple, si le profil est « sexe OR violence », le document Web contenant l'un de ces termes ou ces deux termes sera éliminé par filtrage. Si le profil est « sexe AND violence », le document doit contenir ces deux termes pour être éliminé par filtrage. L'opérateur NOT pourrait être utilisé de la même façon. Si le profil est « sein NOT cancer », les documents qui contiennent le mot « sein », mais pas le mot « cancer » seront éliminés par filtrage. Les documents qui contiennent ces deux termes ou uniquement le mot « cancer » ne seront pas éliminés. Une fois qu'il a repéré un ensemble de documents répondant à la demande, le système peut classer ces documents selon le nombre d'occurrences des termes de recherche que chacun contient.

Le modèle d'espace vectoriel suppose que la requête et chaque document Web sont représentés par des vecteurs de mots-clés. S'il existe « n » mots-clés uniques dans la base de données et la requête, chaque document et le profil sont représentés par un vecteur à n dimensions. La similarité entre la requête et chaque document est une mesure de la proximité des vecteurs à l'intérieur de l'espace à n dimensions. Un certain nombre de mesures de similarité sont utilisées, mais la plus courante est le cosinus. Celle-ci mesure l'angle entre la requête et un document. Une valeur de similarité de cosinus de 1 signifie que la requête et le document sont identiques, tandis qu'une valeur de 0 signifie que les représentations vectorielles sont orthogonales (complètement différentes). L'avantage de ce modèle est, au niveau de l'extraction et du filtrage, qu'il classe les documents par ordre de similarité avec la demande.

Les algorithmes de recherche par chaînes de caractères n'exigent aucun traitement préalable des documents Web à rechercher. Il n'y a pas non plus de suppression des mots vides ni de recherche de radical et aucune structure de fichiers n'est créée. Le texte des documents Web à rechercher est traité comme une suite continue de texte et est exploré « à la volée ». On peut considérer qu'avec ce modèle, la recherche consiste à analyser le document Web en le comparant avec la requête, contrairement à la recherche consistant à analyser la requête en la comparant avec les fichiers à recoupement du document Web. Ces algorithmes peuvent trouver des concordances de chaînes dans ces documents, même si la chaîne est une sous-chaîne. Par exemple, le terme de recherche « sexe » serait trouvé dans la chaîne « unisexe » d'un document Web.

Les algorithmes d'analyse de pages individuelles peuvent également être utilisés pour établir automatiquement des étiquettes d'après le contenu textuel des pages. Dans ce cas, le profil représente la catégorie d'évaluation plutôt que les intérêts d'un utilisateur ou d'un groupe d'utilisateurs.

---

[30] Frakes, William B. et Ricardo Baeza-Yates. 1992. *Information Retrieval: Data Structures and Algorithms*. Englewood Cliffs, New Jersey: Prentice Hall.

L'architecture des systèmes d'analyse de texte comprend généralement trois modules :

- Gestionnaire de profil – gère les profils d'intérêts de divers utilisateurs ou groupes d'utilisateurs. Pour qu'il puisse être utilisé de façon durable, le profil doit être mis à jour de manière à refléter les changements et la précision des intérêts et du vocabulaire.
- Représentation du document - à mesure qu'arrive chaque document, une représentation généralement basée sur des mots-clés est extraite ou générée. Cette représentation indique le contenu du document.
- Algorithme de sélection - la représentation du document est comparée avec le ou les profils d'utilisateur et le document reçoit une valeur numérique représentant sa similarité avec le profil.

#### 3.1.3.1 Création de profils et de représentations de document

*Profils*

Les profils sont des énoncés d'intérêts (positifs ou négatifs) concernant des utilisateurs individuels ou des groupes d'utilisateurs. En règle générale, on utilise des mots-clés ou des expressions pour représenter des catégories d'intérêts. On peut aussi ajouter des coefficients de pondération pour indiquer l'importance relative de chaque mot-clé ou de chaque expression. Les intérêts peuvent être à long terme ou à court terme, statiques ou dynamiques. Les algorithmes d'apprentissage sont nécessaires pour permettre au profil de s'adapter à mesure que le contenu et les intérêts changent au fil du temps.

*Création du profil*

La valeur d'un profil dépend de la sélection de mots-clés ou d'expressions représentant les intérêts de l'utilisateur de façon adéquate. Les éléments à considérer dans la sélection de ces mots-clés représentatifs sont les suivants :

- Les mots-clés ou les expressions du profil doivent avoir une grande efficacité prédictive; autrement dit, les mots-clés doivent apparaître très souvent dans les documents d'intérêt et très rarement dans les autres.
- Des listes pertinentes de mots vides (mots courants) sont utilisées pour éliminer les mots réputés avoir peu d'efficacité prédictive, tels les mots « et », « sont » ou « école », dans un ensemble de données sur l'éducation.
- Les algorithmes de radicaux sont utilisés pour associer des mots de même racine à des radicaux utiles. Par exemple, « programme », « programmer » et « programmation » seront associés au radical « program ».
- Il est possible d'utiliser, dans un profil, des mots et des expressions aussi bien positifs que négatifs. Par exemple, un utilisateur pourrait choisir le terme « artères » comme mot-clé positif dans le cas d'une recherche portant sur le

débit sanguin. Un mot-clé négatif comme « routes » permettrait d'éliminer les documents qui traitent des artères dans le contexte du transport public.

- Les données de l'utilisateur sur la pertinence et l'importance des mots-clés sont essentielles à l'affinage et à la gestion continue des mots-clés d'un profil.
- Les profils contenant de 50 à 100 mots-clés sont ceux qui semblent fonctionner le mieux; en effet, un profil contenant peu de mots omet des mots-clés importants, tandis qu'un profil en contenant trop augmente le niveau de bruit.
- Il est possible d'utiliser des dictionnaires analogiques spécialisés pour compléter la sélection de mots-clés ou d'expressions de l'utilisateur. On peut d'ailleurs créer des dictionnaires analogiques pour des ensembles de documents qui reflètent les relations existant entre les termes de ces documents.
- Des profils d'intérêt préliminaires sont souvent générés à partir de documents types sélectionnés par l'utilisateur.

*Tenue à jour des profils : apprentissage*[31]

Dans le filtrage de contenu, la valeur des profils est directement liée à la corrélation entre le vocabulaire définissant les intérêts de l'utilisateur et le vocabulaire utilisé par les producteurs de contenu. Certaines techniques d'apprentissage sont utilisées pour affiner petit à petit les listes de profil afin qu'elles expriment mieux les intérêts utilisateurs. Il s'agira par exemple d'utiliser les données des utilisateurs ou d'analyser le contenu des pages Web auxquelles l'utilisateur a déjà accédé. Il existe plusieurs catégories de méthodes d'apprentissage que l'on peut appliquer aux profils des utilisateurs :

- Apprentissage direct - l'utilisateur fournit un ensemble de mots-clés ou d'expressions qu'il met périodiquement à jour. L'utilisateur est donc ici directement responsable, et cela exige de sa part un certain effort pour que la méthode soit efficace.
- Apprentissage partiellement direct - le système interprète les commentaires de l'utilisateur sur le degré de pertinence du document présenté par rapport à l'intérêt établi. La participation de l'utilisateur augmente quelque peu pendant le processus, mais celui-ci n'a pas de responsabilité explicite en ce qui concerne les modifications à apporter au profil.
- Apprentissage indirect - le système surveille le comportement de l'utilisateur pour évaluer le succès relatif du filtrage - par ex. impression, création de signets, téléchargement ou utilisation de journaux de site. Cela évite à l'utilisateur d'avoir à intervenir explicitement, mais les changements peuvent être ambigus, car il se peut que la justification de l'intérêt pour certains documents ne soit pas très claire
- Filtres collectifs - le filtre collectif utilise les opinions d'un groupe d'utilisateurs pour faire des recommandations. Le système tient à jour un filtre

[31] W.Lam et K.L.Yu. An Intelligent Adaptive Filtering Agent Based on an On-line Learning Model. Proceedings of ACM SIGIR99 Conference. Berkley, Ca. 1999. 287-288.

commun en fonction des nouvelles données d'un grand nombre d'utilisateurs ayant des intérêts semblables.

*Contenu de pages*

Le contenu d'une page Web est représenté par un ensemble de mots-clés, de la même façon qu'un profil, qui consiste en un ensemble de mots-clés représentant les intérêts de l'utilisateur ou du groupe d'utilisateurs.

*Sélection de mots-clés pour représenter le contenu du document*

Si des algorithmes de recherche par chaînes sont utilisés, le document est visualisé comme une suite de caractères et aucune liste de mots vides ni aucun algorithme de recherche de radicaux ne sont appliquées.

Si un modèle tel que le modèle booléen ou le modèle d'espace vectoriel est utilisé, les mots-clés sont automatiquement extraits du texte du document, les mots vides sont éliminés et la recherche de radical est effectuée; les radicaux trouvés sont stockés dans une structure de fichiers à recoupement. Un coefficient de pondération peut être attribué à chaque radical de mot-clé restant. Le modèle booléen suppose, pour les besoins de l'extraction, un coefficient de pondération binaire. Si le terme apparaît dans le document, le coefficient de pondération est de 1 et s'il n'apparaît pas, le coefficient de pondération est de 0. Toutefois, un coefficient de pondération non binaire peut être utilisé pour établir le classement des documents extraits par le modèle booléen. S'il correspond simplement au nombre d'occurrences du terme dans le document Web, le coefficient de pondération demeure statique jusqu'à ce que le document soit réindexé par le moteur de recherche.

Le modèle d'espace vectoriel peut utiliser des coefficients de pondération binaires ou non binaires. La mesure la plus robuste et la mieux connue pour évaluer la pertinence d'expressions ou de mots individuels apparaissant dans un document et destinés à le représenter est la mesure TF-IDF (*Term Frequency-Inverse Document Frequency*).

La mesure TF-IDF sert à évaluer si les mots-clés extraits du document représentent bien ce document. La même mesure peut être utilisée pour sélectionner certains mots d'un document type afin de les utiliser dans le profil. D'après la mesure TF-IDF, la valeur représentative d'un mot-clé est directement proportionnelle au nombre de fois qu'il apparaît dans le document et inversement proportionnelle au nombre de documents, indexés par le moteur de recherche, dans lesquels ce mot apparaît. Le mot qui apparaît de nombreuses fois dans un document est jugé important pour ce document. Le mot qui apparaît dans de nombreux documents différents n'est probablement pas un bon descripteur de contenu, car il ne peut être utilisé pour établir une distinction entre divers documents.

### 3.1.3.2 Gestion des profils d'utilisateur et des représentations de document

Comme nous l'avons indiqué précédemment, les profils peuvent être statiques ou dynamiques. S'ils sont statiques, les profils sont établis une seule fois. S'ils sont dynamiques, les profils doivent être adaptatifs, c'est-à-dire qu'ils doivent évoluer au fil du temps pour refléter les nouveaux intérêts de l'utilisateur, ainsi que les changements apportés aux documents qui sont offerts. Pour que ces profils soient adaptatifs, il faut qu'il y ait un algorithme d'apprentissage en place.

Les représentations de document sont statiques, à moins que la mesure TF-IDF ne soit utilisée. Une mise à jour continue s'impose, étant donné que le calcul de la valeur représentative d'un terme dépend du nombre connu d'articles indexés dans lesquels apparaît ce terme et que le nombre de documents indexés par le moteur de recherche change continuellement.

#### 3.1.3.3 Utilisation de l'analyse automatique du texte pour filtrer les pages Web

Le filtrage à l'aide de méthodes d'analyse automatique du texte peut être effectué pour répondre à une demande de recherche de l'utilisateur ou à une demande d'exploration générée par l'utilisateur qui a cliqué sur un lien donnant accès à une page. Tout d'abord, le traitement de la demande au niveau du moteur de recherche est basé sur le modèle booléen ou sur le modèle d'espace vectoriel, tel que nous l'avons décrit précédemment.

Une recherche filtrée peut être exécutée si l'on dispose d'un profil qui exprime bien ce que l'utilisateur veut faire bloquer. Dans ce cas, le profil est traité comme une demande et l'extraction est effectuée par le moteur de recherche. On obtient alors un ensemble d'URL répondant au profil. La demande elle-même est ensuite traitée et un ensemble d'URL répondant à cette demande est extrait. L'ensemble d'URL répondant au profil est alors *supprimé* de l'ensemble d'URL renvoyé par la recherche. L'ensemble d'URL ainsi obtenu est envoyé à l'utilisateur. Ceci peut se faire au niveau du moteur de recherche ou au niveau de l'FSI qui fait office de mandataire.

Toutefois, le modèle d'espace vectoriel ne convient pas aux profils dans un système de filtrage conçu pour exclure l'extraction de documents. Pour effectuer un filtrage rigoureux à l'aide de ce modèle, tout document Web dont la similarité de cosinus avec le profil est supérieure à 0 doit contenir au moins un terme du profil. On revient alors au modèle booléen dans lequel les termes du profil sont tous connectés par l'opérateur booléen OR. Ce modèle est généralement plus rapide et coûte moins cher à mettre en œuvre et à exécuter.

L'utilisateur peut parcourir le Web en cliquant sur un lien d'une page Web. Dans ce cas, aucune recherche n'est générée. En fait, c'est une demande d'extraction et de renvoi de la page à l'utilisateur qui est générée. Dans ce cas, il se peut que la page Web n'ait pas été traitée précédemment et on ne sait pas si c'est une page acceptable ou pas. La recherche sérielle par chaînes de caractères peut alors être effectuée dans la page extraite pour s'assurer que celle-ci ne contient aucun des termes du profil. Le filtre doit ici être désactivé au niveau du client ou du FSI qui fait office de mandataire.

*Exécution du filtrage par analyse automatique du texte*

Quoique de nature semblable, ces algorithmes de filtrage peuvent être exécutés de diverses façons :

- Ils peuvent être exécutés à titre d'élément du logiciel installé sur le serveur mandataire du FSI. Le logiciel est exécuté sur les sites Web qui ont été extraits par le serveur mandataire ou qui y sont déjà stockés.
- Ils peuvent être exécutés à un niveau plus précis sur l'ordinateur du client à titre d'application autonome ou dans le contexte d'un navigateur standard.
- Ils peuvent résider sur un site Web hôte.
- Ils peuvent être exécutés par un ou plusieurs agents au niveau du serveur.
- Ils peuvent être exécutés par des agents mobiles ou des robots Web.

*Exemples d'applications qui utilisent le filtrage par analyse automatique du texte*

- La plupart des moteurs de recherche sont dotés d'un mécanisme de filtrage facultatif par le biais duquel l'utilisateur peut demander le blocage des pages qui entrent dans une ou plusieurs des catégories telles que le sexe, la violence, etc.
- Surfwatch— le filtrage par analyse automatique du texte est une des méthodes employées par ce logiciel pour trouver les sites inconvenants et en bloquer l'accès aux enfants. Surfwatch utilise également la méthode de filtrage des URL.
- CyberSitter— utilise le filtrage par analyse automatique du texte pour la plupart de ses blocages. Il utilise également les systèmes d'évaluation PICS et les évaluations de tiers pour filtrer les sites.
- WebChaperone avec iCRT analyse le texte pour déterminer les ratios de comptes de mots, ainsi que la longueur et la structure des mots; il effectue également de l'analyse contextuelle et utilise des coefficients de pondération pour repérer les sites répréhensibles.

### 3.1.4 Méthodes de contrôle des autorisations

Outre les mécanismes de filtrage des demandes de recherche et des résultats de recherche, il existe des mécanismes qui exigent de l'utilisateur autorisé qu'il s'identifie avant que l'accès à un site ou à des données lui soit permis par l'hôte. Ce genre de mécanisme complète la méthode de filtrage en définissant des domaines de documents pour lesquels des privilèges d'accès explicites sont nécessaires. Voici une brève description de quelques-unes de ces technologies pour ce qui est de l'accès à Internet.

*Chiffrement* – Les systèmes de chiffrement standard peuvent être utilisés pour fournir des documents à un site client lorsqu'un accès restreint à ces documents s'impose; exemple : des documents pour adultes ne convenant pas aux enfants. Les systèmes de chiffrement, tel l'ICP (infrastructure à clés publiques), ou les algorithmes de clés privés, exigent que le client possède une clé valide pour pouvoir effectuer le déchiffrement.

*Noms de connexion et mots de passe* – Des noms de connexion et des mots de passe standard peuvent être attribués à des utilisateurs autorisés de sites contenant des données de diffusion restreinte. Les utilisateurs qui désirent accéder aux données de ces sites ou transférer des données à partir de ces sites doivent d'abord obtenir un nom de connexion et un mot de passe pour pouvoir accéder à ces sites.

*Carte de crédit ou vérification de l'âge* – Un site hôte peut exiger de l'utilisateur qu'il fournisse un numéro de carte de crédit valide ou une autre preuve établissant qu'il a l'âge requis pour pouvoir accéder à un site. On part ici du principe que seules les personnes de plus de 18 ans détiennent une carte de crédit valide. L'Australie[32], par exemple, propose une validation de la carte de crédit pour vérifier si la personne qui demande à accéder à des documents pour adultes a au moins 18 ans. Il existe maintenant un logiciel[33] qui peut vérifier l'âge seul sans autre donnée d'identification.

*Biométrie et matériel* - Des algorithmes de biométrie et des périphériques permettant d'identifier les utilisateurs de façon unique sont actuellement mis au point; par exemple, la lecture des empreintes digitales, la lecture des empreintes rétiniennes et l'empreinte vocale utilisent une combinaison d'éléments matériels et d'éléments logiciels pour reconnaître chaque utilisateur. Un exemple de méthode algorithmique est l'utilisation du rythme de frappe[34] du mot de passe pour identifier l'utilisateur de façon unique.

### 3.1.5 Repérage des activités

Les serveurs consignent bon nombre de données relatives à l'utilisation d'Internet. Chaque accès sollicité par le biais du serveur est enregistré. Cet enregistrement comprend les éléments suivants : adresse du client, date et heure, adresse de la page du serveur à laquelle le client a accédé, nombre d'octets, erreurs générées par le serveur ou par un script. Ces fichiers journaux, qui sont généralement utilisés pou équilibrer les charges et détecter les habitudes d'utilisation, peuvent également servir à surveiller les activités individuelles des clients.

De la même façon, il est possible d'enregistrer et d'analyser les activités de l'utilisateur, de la frappe à la commande d'application, pour contrôler son comportement, ainsi que de prendre périodiquement des instantanés d'écran pour enregistrer des conversations en ligne, du courrier électronique et des activités de traitement de texte.

---

[32] *Online Services Content Regulation.* [En ligne]. DFSIonible à : http://www.aba.gov.au/what/online/restricted.htm [janvier 2000]

[33] ZeroKnowledge. [En ligne]. DFSIonible à : http://www.zeroknowledge.com [mars 2000]

[34] NetNanny Software International Inc. 1994-1998. *BioPassword: undeniably identified.* [En ligne]. DFSIonible à : http://www.biopassword.com/docs/BioPassword.PDF [janvier 2000]

## 3.2 Niveau applications

### 3.2.1 Applications de navigation pour enfants

Il est possible de développer des applications de navigation à l'intention des jeunes utilisateurs. Ces applications peuvent offrir des stratégies de recherche simplifiées et des graphiques plus conviviaux, supprimer les annonces publicitaires et fournir une fonction de filtrage et des domaines de recherche sûre d'une façon qui soit transparente pour l'utilisateur.

#### 3.2.1.1 Utilisation d'applications de navigation pour enfants

Les méthodes utilisées par ces applications sont les suivantes :

- Utilisation d'une base de données de sites « sûrs ». Les enfants ne sont autorisés à accéder qu'à une base de données de sites préapprouvés. L'accès à ces sites s'effectue généralement par le biais d'une interface portail, d'icônes ou de listes de menus.
- Utilisation d'URL d'une liste « noire » ou de mécanismes de filtrage par mots-clés. Les enfants ne peuvent accéder aux URL qui figurent sur la liste noire. Ces URL sont des sites qui ont été jugés inconvenants pour les enfants. Les URL de listes noires ne sont pas extraits d'Internet. Lorsqu'ils recherchent des sites, les enfants ne peuvent utiliser les mots-clés susceptibles de renvoyer des sites inappropriés.

#### 3.2.1.2 Exemple d'applications de navigation pour enfants

SurfMonkey[35] est un très bon exemple de navigateur autonome conçu pour les enfants. Il utilise des listes et des mots-clés pour empêcher les enfants d'accéder à divers éléments du Web : pages Web, courrier électronique, salons de bavardage et groupes de discussion.

### 3.2.2 Moteurs de recherche et portails axés sur les intérêts des enfants

L'idée est d'utiliser, dans ces deux cas, une passerelle de tiers qui donne accès au contenu du Web. Les portails conçus pour les enfants sont des sites d'accès au Web qui essaient de fournir un domaine de sites sûrs que l'utilisateur peut explorer. Du moment qu'il passe par le portail, l'utilisateur ne peut visualiser qu'un ensemble de domaines présélectionnés du Web.

#### 3.2.2.1 Utilisation des moteurs de recherche et des portails destinés aux enfants

[35] *SurfMonkey*. [En ligne]. DFSIonible à : www.surfmonkey.com [mars 2000]

Bon nombre des moteurs de recherche les plus utilisés, comme Lycos et Infoseek, offrent des modes d'accès spécialement conçus pour les enfants. Ces produits utilisent une ou plusieurs des méthodes suivantes :

- Obstruction de mots-clés de recherche.
- Filtrage des résultats.
- Répertoire de « bons » sites.

#### 3.2.2.2 Exemples de moteurs de recherche et de portails destinés aux enfants

**InfoSeek** — offre des liens intitulés Disney.com et Kids, qui sont des domaines d'exploration sûrs pour les enfants.
**Lycos** — offre également un lien intitulé Kids, que les enfants peuvent explorer en toute sécurité.
**Yahooligans**[36] — portail/moteur de recherche conçu pour les enfants par Yahoo! Inc.

### 3.2.3 Applications mandataires

Un serveur Web mandataire est un module logiciel qui est intégré au logiciel du serveur et qui fait office d'intermédiaire entre les clients et le serveur (et Internet). Lorsque le logiciel mandataire est installé, toutes les demandes d'accès HTTP passent par le module mandataire avant d'être envoyées au serveur pour être traitées sur Internet. Sans mandataire, toutes les demandes HTTP des clients vont directement dans le serveur et sont mises en communication avec le site de destination.
Le mandataire gère toutes les demandes et décide si elles doivent être exécutées. Si elles répondent aux conditions définies dans le mandataire, les demandes sont alors transférées au serveur pour être traitées. Étant donné que les utilisateurs individuels peuvent, dans la plupart de navigateurs, « désactiver » le mandataire dans les préférences de l'utilisateur, le serveur peut fermer toutes les connexions vers l'extérieur, sauf vers le mandataire, de sorte que seul le serveur mandataire puisse soumettre les demandes sur Internet.

En règle générale, le module mandataire gère la mise en antémémoire et l'enregistrement local des documents demandés, et ce, pour améliorer l'efficacité des opérations du serveur. Le mandataire peut donc être utilisé pour analyser le contenu de ces documents afin de déterminer s'il peut être envoyé au client.

Une mini-application Java est un programme Java conçu pour être intégré à un document HTML sur le site serveur, acheminé à travers un réseau et exécuté sur le site client à l'aide d'un navigateur Web. Les modules mandataires comme SurfinGate[37] peuvent être utilisés pour évaluer les mini-applications et décider quelles sont celles qui peuvent être envoyées au client d'après des critères de principe.

---

[36] *Yahooligans*. 1994-2000. [En ligne]. dFSIonible à : www.yahooligans.com [janvier 2000]
[37] Stewart, John. (April 1997). *Proxy Servers to Filter Content*. [En ligne]. DFSIonible à : http://webserver.cpg.com/ws/2.3/ [mars 2000]

*Technologies de filtrage basées sur l'antémémoire*

Les demandes HTTP du client au serveur nécessitent l'exécution de plusieurs étapes pour chaque transaction :

- Le client se connecte au serveur.
- Le client envoie une demande de document.
- Le serveur répond généralement en envoyant le document au client. Une fois le document reçu, le serveur coupe la connexion.

La mise en antémémoire désigne l'enregistrement d'une copie du document sur un disque local ou dans une mémoire locale, et ce, pour réduire le temps d'attente des demandes subséquentes visant le même document. Autrement dit, la prochaine fois qu'il sera demandé, le document pourrait provenir directement du disque local, ce qui évite de solliciter à nouveau le serveur de l'URL pour l'extraction et l'envoi du document. Cette mise en antémémoire peut se faire au niveau du serveur du FSI, de l'ordinateur client ou des deux. Au niveau du FSI, les documents en antémémoire de plusieurs utilisateurs peuvent être conservés dans une antémémoire générale : si l'on part du principe qu'un certain nombre d'utilisateurs demanderont à accéder à ces mêmes documents, cette méthode accélère considérablement le traitement des demandes. En même temps, la mise en antémémoire des documents peut servir à filtrer les données de façon plus efficace.

Les applications utilisant l'antémémoire sont conçues pour gérer la mise en antémémoire des pages Web et permettre l'accès à ces pages. Elles peuvent être utilisées pour répondre aux demandes HTTP à partir de l'antémémoire locale (si possible), pour exécuter les fonctions d'authentification et vérifier les étiquettes et les autres exigences de filtrage de contenu. Les applications utilisant l'antémémoire sont plus légères que les serveurs mandataires et donc plus faciles à adapter. Le plus grand avantage de ces applications[38] est qu'elles accélèrent la livraison des pages Web, mais elles peuvent également améliorer le filtrage du contenu.

Dans ce cas, le filtrage s'effectue selon une recherche sérielle par chaîne de caractères, étant donné qu'aucune structure de fichiers à recoupement n'est créée au site de l'antémémoire. Ce genre de filtrage convient dans les deux situations suivantes :

- Les pages ont été mises en antémémoire à la suite d'une demande de recherche. La recherche sérielle par chaînes de caractères dans ces pages s'effectue à titre de filtrage de deuxième couche, c'est-à-dire au-dessus du filtrage faisant appel au modèle booléen ou au modèle d'espace vectoriel.
- Les pages ont été mises en antémémoire à la suite d'une demande d'accès à un lien sélectionné par l'utilisateur.

[38] *CacheFlow*. 1998, 1999. [En ligne]. DFSIonible à : www.cacheflow.com [janvier 2000]

*Agents*

Un agent est un programme autonome qui a un but et qui agit sur son environnement pour atteindre ce but[39]. La notion d'autonomie est importante, car l'agent possède un ensemble de règles qui déterminent si le contenu d'un site donné est acceptable ou non et il y a des milliers d'agents qui peuvent être déployés en même temps pour évaluer l'information contenue dans chaque site et envoyer une simple réponse. Les agents peuvent éventuellement communiquer entre eux et fonctionnent généralement de façon indépendante.

Les **agents de filtrage de la recherche**[40] interviennent généralement sur les résultats de la recherche au niveau du mandataire du FSI. Ces agents peuvent être définis pour plusieurs profils et traitent simultanément les résultats d'une recherche donnée. Les résultats des agents sont stockés par un programme pilote qui utilise les réponses individuelles pour éliminer les pages indésirables.

Les **robots filtreurs**[41] sont des agents de classification automatisés qui évaluent les nouveaux documents à des sites distants dès qu'ils sont diffusés sur le Web. Le profil de chaque utilisateur ou groupe d'utilisateurs est géré par un robot séparé. Le client extrait les documents en communiquant avec un serveur de recommandations.

*Exploration du Web (découverte)*

L'exploration du Web est le processus proactif de recherche de ressources Web. Il s'agit en fait de la recherche active de pages associées à un ensemble de sujets prédéfini, et ce, pour les inclure ou les exclure. Plutôt que de faire de l'indexation ou d'utiliser des index de toutes les pages Web connues, le robot Web recherche dans son URL les liens éventuels donnant accès à d'autres URL, recherchant ceux qui sont les plus susceptibles de mener à des pages pertinentes et excluant les grandes sections de pages non pertinentes. Certaines études[42] démontrent que la recherche par sujet s'avère très efficace pour établir des collections de documents Web de grande qualité.

---

[39] M. Wooldridge. Intelligent Agents. In *Multiagent Systems*, Ed. G. Weiss. MIT Press, Cambridge, USA. 1999. p. 27-78.

[40] Agha, G. and N.Jamali. 1999. *Concurrent Programming in MultiAgent Systems.* MIT Press, Cambridge, Mass.

[41] Sarwar, B., J.Konstan, A.Borchers, J.Herlocker, B.Miller, et J.Riedl. 1998. Using filtering agents to improve prediction quality in GroupLens Research Collaborative Filtering System. Proc. of CSCW 98 Seattle Washington. 345-354

[42] S.Chakrabarti, M.vanden Berg, and B.Dom. 1999. Focused crawling: a new approach to topic- specific Web resource discovery. In *Proceedings of WWW8 Conference*. Elsivor Science Press. P. 545-562.

### 3.2.4 Applications de surveillance des activités

Il existe maintenant des applications qui surveillent et enregistrent les activités liées à Internet pour que les parents puissent voir à quoi accèdent leurs enfants. Ces applications peuvent être exécutées au niveau du FSI ou du client. Le FSI peut facilement consigner toutes les activités des utilisateurs par le biais de son serveur. Les applications offertes au niveau du client consignent les activités particulières de l'utilisateur et préparent des vues de ces activités afin qu'elles soient analysées. Ces applications utilisent certaines ou l'ensemble des méthodes suivantes :

- Enregistrement de l'emploi de certains mots-clés ou de certaines expressions dans les recherches.
- Consignation de tous les URL visités.
- Limite du temps d'exploration.
- Enregistrement périodique d'un instantané d'écran.
- Saisie des graphiques mis en antémémoire.
- Utilisation de fichiers témoins (cookies) pour l'enregistrement des données sur les activités du client.

Exemples :

**NetNanny**—surveille et consigne les sites qui sont visités, les programmes qui sont utilisés et les termes et expressions qui sont tapés et/ou reçus, selon le choix de l'utilisateur.
**CYBERsitter**—tient un historique complet de toutes les activités liées à Internet, dont les tentatives d'accès à des documents bloqués.
**Bess**—comporte également un "logiciel de rapport" pour contrôler les activités liées à Internet.
**Smart Alex ICU** – surveille toutes les activités Internet en ligne et hors ligne à l'aide d'instantanés d'écran.

### 3.2.5 Applications limitant l'accès aux données

Les applications qui résident sur le site hôte peuvent être élaborées de façon à ne permettre qu'aux utilisateurs autorisés d'accéder aux données ou aux services offerts sur ce site. Les données peuvent être chiffrées de sorte que seuls les utilisateurs autorisés puissent les déchiffrer et les visualiser. Voir la section 3.1.4 pour avoir plus de détails.

### 3.2.6 Applications autres que des applications HTTP

Bien que les sites FTP, le courrier électronique et d'autres données non HTTP soient accessibles par le biais du navigateur, il est fort probable que les applications non HTTP puissent être utilisées en dehors de l'environnement navigateur-serveur pour accéder à des données. Des applications ont été développées exclusivement pour filtrer ces types de données. Ces applications peuvent être autonomes ou incorporées en tant que fonction dans un logiciel de filtrage plus général.

*Courrier électronique* - Les applications de filtrage du courrier électronique sont chargées de filtrer les messages-poubelle et le contenu du courrier électronique. L'envoi de ces messages-poubelle, ou pollupostage, consiste à inonder avec la même copie d'un message électronique, souvent de la publicité, le plus de comptes de courriel possible. Les listes de pollupostage sont souvent générées par la lecture d'articles Newsnet, la recherche d'adresses Web et l'accès à des listes de courrier électroniques pour d'autres besoins. Les listes de pollupostage peuvent comprendre non seulement des adresses électroniques de particuliers, mais aussi des listes publiques ou privées comme celles utilisées pour les groupes de discussion. Le système de filtrage des messages-poubelle utilise des règles pour lire les en-têtes des messages entrants afin d'éliminer les messages susceptibles d'être des messages-poubelle. Par exemple, le domaine de l'expéditeur et le contenu des champs From (De) ou Subject (Objet) sont souvent utilisés.

Le filtrage du contenu est une inspection plus précise du contenu du message pour déterminer si le courrier électronique peut être livré. La plupart des fonctions de filtrage de contenu utilisent un profil de mots-clés qui est comparé avec le contenu du message, comme dans le cas du filtrage du contenu des pages Web. Le courrier électronique rejeté ou suspect peut être réacheminé dans un dossier dont l'accès est protégé par un mot de passe.

Les applications peuvent également surveiller le courrier électronique pour détecter du matériel choquant dans les messages sortants, surtout lorsqu'ils sont associés à un serveur mandataire. Ces applications vont du simple filtrage des messages basé sur des mots-clés au contrôle plus poussé du contenu. Pour une surveillance plus étroite, les applications de courrier électronique comme *Email for Kids*[43] permettent aux parents d'exercer un contrôle sur les messages entrants et les messages sortants, et ce, pour surveiller le contenu des messages, les destinataires et les expéditeurs, ainsi que pour établir des règles à ce sujet.

*Serveurs de nouvelles* – le filtrage des serveurs de nouvelles, comme c'est le cas de UseNet, s'effectue en grande partie au moyen de deux technologies de base qui sont : les listes de groupes de nouvelles acceptables ou non acceptables pour bloquer l'information au niveau du groupe de nouvelles, et le filtrage basé sur les mots-clés.

*FTP* – il est possible d'empêcher raisonnablement les transferts de fichiers en interdisant tout accès ftp ou en contrôlant les sites auxquels l'accès est autorisé. Les sites individuels

[43] *Email for Kids*. [En ligne]. DFSIonible à : http://www.email-connection.com [janvier 2000]

peuvent limiter l'accès en utilisant l'une ou l'autre des technologies de contrôle d'accès, comme l'id-utilisateur et le mot de passe.

*Telnet* – étant donné que Telnet permet à l'utilisateur d'accéder à distance à son propre compte sur un ordinateur distant, le principal mécanisme de contrôle consiste à interdire l'accès Telnet au moyen d'un pare-feu.

*Groupes de discussion, salons de bavardage et applications de messagerie instantanée* - le contrôle de l'accès à ces applications ou aux listes de groupes de discussion acceptables est très simple. Il suffit de développer des applications de type ICQ pour faire partie d'une liste de groupes ou d'une liste de participants acceptables.

Ces fonctions de contrôle sont souvent intégrées à d'autres fonctions de contrôle d'applications plus importantes comme NetNanny ou SurfMonkey.

## 4. Évaluation des types de technologies de filtrage

### 4.1 Technologies de base

#### 4.1.1 Étiquetage de sites

Avantages

- Un système d'évaluation comportant des couches de classification permet normalement une utilisation plus subtile de l'étiquette. Exemple : des résultats de filtrage en fonction de l'âge ou du degré de violence.
- Les utilisateurs peuvent compter sur des sources fiables pour classifier le contenu de façon juste.
- Les systèmes d'évaluation peuvent être conçus ou adaptés pour répondre à certains besoins.
- Si les systèmes d'évaluation sont ouverts, il est alors possible d'en utiliser conjointement plusieurs. Autrement dit, une application pourrait envoyer une demande d'étiquette à plus d'un bureau d'étiquettes, par exemple à un bureau national et à un bureau international.
- L'utilisation de systèmes d'évaluation offre aux applications de filtrage souplesse et uniformité.
- Sécurité and authentification - les étiquettes peuvent comprendre une signature cryptographique ou numérique de sorte que le logiciel ou l'utilisateur puisse vérifier l'authenticité de l'étiquette.

Inconvénients

- Il est actuellement difficile d'analyser automatiquement le contenu d'images vidéo et d'éléments sonores.
- L'efficacité de l'étiquetage dépend surtout de la catégorisation humaine.
- Les étiquettes sont intrinsèquement biaisées. Elles refléteront toujours l'idéologie du groupe qui les a créées.
- L'étiquetage de parties importantes du Web revient cher et est une tâche de longue haleine.
- Il est presque impossible de tenir les étiquettes à jour, surtout dans le cas des sites qui changent de contenu. Une fois qu'un site a été étiqueté, le fournisseur de contenu peut changer le contenu sans modifier l'étiquette.
- L'étiquetage des documents virtuels est impossible. Ce sont des pages dont le contenu est généré à la volée.
- La valeur des sites Web étiquetés par les producteurs même est douteuse.
- Granularité des systèmes d'évaluation : si l'on a un trop grand nombre de catégories, il est difficile d'attribuer des cotes de façon uniforme. Si l'on n'a pas assez de catégories, les cotes sont indifférenciées. Par exemple, la catégorie « grossièretés » ne différencie pas les termes racistes des termes explicitement sexuels.

- Le fait de recourir à un bureau d'étiquettes ou à un tiers ralentit les réponses. On peut cependant utiliser certaines méthodes pour minimiser cet effet, notamment conserver des copies des étiquettes au niveau local et effectuer des demandes en parallèle.
- L'utilisation d'étiquettes HTML intégrée exige que l'on fasse confiance au producteur des étiquettes.
- Si elle est séparée du contenu du document, l'étiquette ne pourra, dans certaines situations, plus être utilisée Exemple : le fait de transférer un document d'un URL à un autre a pour effet de le « désétiqueter ».

### 4.1.2 Listes d'URL

*Listes « noires »*

Avantages

- Elles sont faciles à réaliser.

Inconvénients

- La qualité et l'intégralité de ces listes sont incertaines.
- Les URL sont faciles à changer.
- Les sites miroir peuvent masquer l'URL réel.
- La mise à jour de ces listes est une tâche colossale.

*Listes « blanches »*

Avantages

- Faciles à réaliser.
- Protection robuste.
- Domaines « sûrs ».

Inconvénients

- Qualité
- Exclusion de nombreux sites pouvant être utiles.

### 4.1.3 Analyse automatique du texte

Avantages

- Les sites Web peuvent être étiquetés facilement.

- Les mots-clés et les expressions à rechercher peuvent être choisis de façon à refléter les préférences de l'utilisateur.
- Cette méthode peut être utilisée pour analyser du texte généré « à la volée ».
- Les pages Web auxquelles accède l'utilisateur sont toutes analysées.

Inconvénients

- Les résultats sont médiocres : le contexte du mot ou de l'expression n'est pas pris en compte. Par exemple, si le mot-clé « sein » est utilisé pour éliminer les sites pornographiques, les sites traitant du cancer du sein seront également éliminés.
- Les images, les vidéos et les autres formes de données non textuelles sont très difficiles à analyser.
- Les listes de mots-clés et d'expressions de l'utilisateur doivent être mises à jour pour refléter les nouveaux intérêts de celui-ci, ainsi que les changements au niveau de la terminologie utilisée dans les documents Web.

### 4.1.4 Méthodes d'autorisation

*Chiffrement*

Avantages

- Permet à certains utilisateurs d'installations partagées d'accepter des documents susceptibles de ne pas convenir aux autres utilisateurs de ces installations.
- Les systèmes de chiffrement sont aisément disponibles.

Inconvénients

- Les documents peuvent être laissés sur le disque de l'utilisateur sous une forme non chiffrée.
- Les utilisateurs doivent conserver leur clé et la protéger.

*Noms de connexion et mots de passe*

Avantages

- L'hôte du site est chargé d'autoriser l'accès à ses documents.
- L'utilisation d'un mot de passe est une méthode connue et éprouvée.

Inconvénients

- Les utilisateurs choisissent généralement des mots de passe qui sont, surtout pour ceux qui les connaissent, faciles à deviner (nom de leur animal familier, variante de leur adresse, dates de naissance etc.).
- L'utilisateur qui choisit un mot de passe moins évident l'inscrit souvent sur un bout de papier qu'il laisse près de son ordinateur.
- Pour être efficaces, les mots de passe doivent être changés fréquemment.
- Les utilisateurs qui détiennent plusieurs mots de passe n'en utilisent souvent qu'un ou deux.

*Carte de crédit comme preuve d'âge obligatoire*

Avantages

- Aucune installation nécessaire du point de vue de l'utilisateur ou de l'administration.
- Peut sécuriser l'accès.

Inconvénients

- Il est très facile pour un utilisateur de moins de 18 ans d'obtenir un numéro de carte de crédit valide.

*Biométrie et matériel*

Avantages

- Permet d'identifier l'utilisateur de façon unique.
- Élimine la nécessité d'avoir à changer souvent de mot de passe.

Inconvénients :

- Les solutions basées sur le matériel coûtent encore cher.

### 4.1.5. Repérage des activités

Avantages

- Facilité de collecte de l'information.

Inconvénients

- Il peut être difficile d'identifier l'utilisateur réel.

## 4.2 Applications

### 4.2.1 Navigateurs pour enfants

Avantages

- Possibilité d'avoir des interfaces conçues pour les enfants.
- Pas besoin d'avoir beaucoup d'expérience ni de connaissances dans le domaine pour pouvoir utiliser le système.
- L'utilisateur ne peut « contourner » les contrôles.
- L'utilisateur n'est informé que du domaine et des activités fournies par le navigateur.

Inconvénients

- Les connaissances nécessaires à l'utilisation de ce logiciel ne sont peut-être pas suffisantes pour pouvoir utiliser d'autres navigateurs plus standard.
- Limitent peut-être trop certains enfants.

### 4.2.2. Portails et moteurs de recherche axés sur les intérêts des enfants

Avantages

- Prédéfinissent un domaine de connaissances « sûr ».
- Combinent les sites les plus utiles et les moteurs de recherche en un guide homogène explorable d'un seul clic.

Inconvénients

- Le filtrage par mot-clé n'est pas très efficace. Les deux premières recherches à l'aide de deux grands moteurs de recherche conçus pour les enfants ont renvoyé des documents graphiques de nature sexuelle.
- Les liens qui partent des sites extraits, surtout des interfaces portails, ne peuvent pas être filtrés.

### 4.2.3. Applications mandataires

Avantages

- Peuvent contrôler tous les accès à Internet obtenus par le biais du serveur.

Inconvénients

- Les utilisateurs peuvent les contourner assez facilement.

### 4.2.4. Applications d'autorisation d'accès

Avantages

- Permettent à certains utilisateurs d'installations partagées d'accepter des documents susceptibles de ne pas convenir aux autres utilisateurs de ces installations.
- L'hôte du site est chargé d'autoriser l'accès à ses documents.
- Peuvent éventuellement utiliser un système d'identification, comme une carte de crédit, pour valider l'âge, plutôt que d'avoir recours à un processus d'inscription qui consigne les données d'identification personnelles.

Inconvénients

- Les documents peuvent être laissés sur le disque de l'utilisateur sous une forme non chiffrée.
- Les utilisateurs doivent conserver leur clé et la protéger.
- Les solutions matérielles coûtent actuellement très cher.
- Les utilisateurs choisissent en général des mots de passe que les autres peuvent facilement trouver.
- Pour être efficaces, les mots de passe doivent être souvent changés.
- Il est très facile, pour l'utilisateur de moins de 18 ans, d'obtenir un numéro de carte de crédit valide.

### 4.2.5. Moniteurs d'activités

Avantages

- Fournissent un historique des activités, historique que les parents peuvent utiliser pour s'assurer que leurs enfants n'accèdent pas à des documents inappropriés.

Inconvénients

- Il faut passer beaucoup de temps pour déterminer un mauvais usage quelconque.

- N'empêche pas les utilisateurs d'accéder à du matériel inapproprié.
- Peut aller à l'encontre du respect de la vie privée des utilisateurs.

#### 4.2.6. Filtrage dans le cas des applications non HTTP

Avantages

- Une grande partie du transfert de fichiers s'effectue à l'aide de ces applications.

Inconvénients

- Le filtrage ou le blocage des données propres à ces applications exige normalement des applications séparées.
- Les utilisateurs des navigateurs peuvent souvent contourner les contrôles du serveur en utilisant des applications non HTTP.

## 5. Site où s'opère le filtrage

Les activités de filtrage ont lieu avant la recherche comme telle ou une fois la recherche terminée, mais avant que le document soit présenté à l'utilisateur. Du point de vue technologique, ce traitement peut être exécuté sur le site du FSI ou sur les ordinateurs clients. Le choix du lieu d'hébergement du logiciel doit être basé sur d'autres facteurs : contrôle individuel, opinion collective ou opinion personnelle, responsabilité quant à la création de listes, de mots-clés et d'étiquettes, responsabilité quant aux mises à jour, analyse des risques. Nous aborderons, dans cette section, les avantages que comporte l'hébergement des mécanismes de filtrage au site client individuel, ainsi qu'au site du FSI. Il ne s'agit pas de choisir entre l'une ou l'autre des situations; en fait, une combinaison de mécanismes coordonnés sur les deux sites offre probablement les meilleures caractéristiques des deux options et davantage de souplesse.

### 5.1 Mécanismes autonomes (ordinateur client)

Plusieurs mécanismes sont offerts au niveau du client :

- Surveillance des activités.
- Navigateur spécial.
- Filtrage des mots-clés ou des expressions avant la recherche.
- Filtrage utilisant l'antémémoire et basé sur les URL, les étiquettes ou le contenu.

*Filtrage, au niveau du client, des documents mis en antémémoire*[44]

Les applications du client peuvent examiner le contenu des données extraites d'Internet après que celles-ci ont été téléchargées dans l'antémémoire de l'ordinateur client et avant que le navigateur ne les affiche. Le filtrage peut être basé sur des listes d'URL particulières stockées dans l'ordinateur client, sur l'examen des mots-clés des documents ou sur les données d'étiquetage des pages individuelles. Il existe une autre méthode du même genre qui consiste à télécharger les documents et à demander en même temps à un tiers les étiquettes des pages téléchargées afin de procéder au filtrage au niveau du client.

Avantages

- Des profils personnalisés et confidentiels très précis peuvent être utilisés.

Inconvénients

- Des documents répréhensibles peuvent déjà se trouver dans l'ordinateur client et d'autres applications pourraient y accéder facilement.

[44] McRae, Philip et al. (June 1998). *Blocking Content on the Internet: A Technical Perspective* [En ligne]. DFSIonible à : http://www.cmis.csiro.au/projects+sectors/blocking.pdf [janvier 2000]

- Les graphiques, en particulier, sont très difficiles à bloquer, puisque ce sont des algorithmes de texte qui sont utilisés.

## 5.2 Mécanismes du FSI

Le FSI peut offrir à ses abonnés des services à valeur ajoutée en fournissant, à son niveau, des filtres à l'aide de pare-feu ou de serveurs mandataires. Les pare-feu sont des passerelles qui contrôlent tout le trafic en direction ou en provenance du système hôte et d'Internet. Le logiciel installé au niveau du pare-feu peut être configuré de façon à rejeter certaines catégories d'accès pour tous les utilisateurs du système.

Un serveur mandataire est une application côté serveur qui fonctionne avec le logiciel du serveur à titre de canal des demandes des clients. Le navigateur du client doit être configuré de façon à utiliser le serveur mandataire. Le logiciel mandataire fait office d'intermédiaire dans le processus d'accès aux pages Web. Toutes les demandes des clients passent par le serveur mandataire et les résultats extraits d'Internet passent également par ce serveur avant d'être envoyés à l'utilisateur. Les mécanismes de contrôle, qui sont généralement exécutés à l'aide d'un serveur mandataire, sont les suivants :

- Application de filtres d'étiquettes.
- Filtrage des résultats de recherche par liste ou par contenu.
- Mise à disposition d'une base de données de sites de recherche « sûrs ».
- Mise à disposition de sites portails conçus pour les enfants.

En règle générale, le serveur mandataire met en antémémoire ou enregistre au niveau du FSI les pages Web extraites. Les données mises en antémémoire permettent ainsi de réduire le temps de transmission et de téléchargement ainsi que la congestion et peuvent être utilisées pour filtrer les données avant qu'elles ne soient envoyées à l'utilisateur. Le mandataire du FSI peut exécuter plusieurs tâches liées au filtrage :

- Mettre en antémémoire certaines hiérarchies de pages en utilisant des listes.
- Vérifier par rapport au site source si la page mise en antémémoire est à jour avant de l'envoyer au client.
- Vérifier les étiquettes associées aux pages mises en antémémoire.
- Refuser d'envoyer au client certaines pages de l'antémémoire d'après des listes.
- Analyser le contenu des pages pour déterminer s'il faut envoyer ou supprimer celles-ci.

La plupart des FSI offrent un navigateur qui est préconfiguré pour afficher, lorsqu'il est lancé, un site portail à titre de page d'accueil par défaut de l'utilisateur. Le client peut, dans tous les cas, configurer son navigateur pour le faire passer par le serveur mandataire du FSI. L'utilisation de ce serveur mandataire empêche les clients d'aller directement sur Internet, car toutes les demandes sont traitées par le biais de ce serveur. Le logiciel

mandataire peut enregistrer ou mettre en antémémoire les résultats qui peuvent alors être filtrés avant d'être envoyés au client.

*Avantages*

- Élimine la nécessité d'installer un logiciel séparé sur l'ordinateur client.
- Des applications parallèles et à fort pourcentage de calculs peuvent être utilisées au niveau du FSI.
- Le filtrage au niveau de l'antémémoire du FSI peut réduire la quantité de traitements nécessaires.
- Le FSI peut tenir à jour une vaste base de données d'étiquettes et/ou de listes collectives.
- Le FSI se charge de la mise à jour des listes.
- Le FSI peut élaborer des stratégies de recherche proactives pour cataloguer les nouveaux sites.
- Le FSI peut filtrer l'information de façon transparente pour l'utilisateur.

*Inconvénients*

- Les sites peuvent être facilement renommés et, de ce fait, ne pas concorder avec les noms figurant dans la liste du mandataire.
- Les services de traduction peuvent produire des versions contenant des mots qui ne figurent pas dans le profil; ces versions ne seront donc pas filtrées efficacement par les algorithmes de mots-clés.
- Les listes doivent inclure le nom de domaine et l'adresse Internet IP.
- Les applications ne fonctionnent pas toutes bien lorsqu'elles passent par un serveur mandataire et cela peut nuire à leur performance.
- Les technologies du pousser contournent généralement les vérifications du mandataire et livrent directement le contenu aux sites des utilisateurs.
- Tout le monde n'accède pas à Internet par le biais d'un FSI.
- Les sites miroir, autres URL de certains sites, doivent être inclus dans toutes les listes, puisque le même contenu peut avoir plusieurs URL.
- À mesure qu'augmente le trafic sur Internet, les serveurs mandataires deviennent de véritables goulots d'étranglement et peuvent réduire la performance.
- Si les liens figurant sur les pages Web externes n'utilisent pas le numéro de port standard, les demandes visant ces pages ne seront pas interceptées.

## 6. Résumé et recommandations

En résumé, on dispose d'un certain nombre de moyens pour contrôler l'accès au contenu, moyens qui reposent sur une ou plusieurs des technologies de base sous-jacentes. Étant donné que ces applications de contrôle et ces technologies de base peuvent être combinées et que la plupart peuvent être utilisées au niveau du FSI ou du client ou encore au niveau des deux, il n'y a pas de recommandation précise à faire quant à la meilleure méthode ou au meilleur lieu d'utilisation. Quoi qu'il en soit, les utilisateurs doivent être informés et participer au processus.

Voici un récapitulatif des possibilités qu'offrent ces technologies de base :

- Les systèmes d'étiquetage de sites sont les plus souples et peut-être les plus prometteurs. Il revient au FSI ou au client (ou aux deux) d'utiliser les étiquettes qui ont été attribuées.
- L'utilisation de listes d'URL constitue la méthode la plus efficace pour contrôler les domaines d'accès. Cette méthode convient particulièrement bien pour créer des sites destinés aux enfants. Elle n'offre cependant pas toute la souplesse des étiquettes et le Web s'agrandit si rapidement qu'il est très difficile de garder des listes à jour.
- L'analyse automatique précise du contenu des sites Web est problématique dans le meilleur des cas, compte tenu des fantaisies du langage naturel, des problèmes de filtrage des divers langages et de la difficulté qu'il y a à déterminer le contenu des graphiques et des images. Toutefois, l'utilisation de cette technologie pour *faciliter* l'étiquetage des sites d'après les méthodes de catégorisation de texte s'avère d'une certaine manière prometteuse.
- Le droit d'accès peut être efficace comme filtre inverse, car il limite l'accès à un site donné.
- La méthode de repérage d'activités ne permet que de surveiller ce qui a été fait; elle ne permet pas de filtrer quoi que ce soit.

Même si l'on considère qu'ils ne font pas partie de la technologie de base, les robots Web peuvent faire office d'agents d'évaluation qui classent les sites de façon proactive d'après des algorithmes d'analyse de contenu. Bien qu'elle n'ait pas encore fait preuve de grande précision, cette méthode mérite d'être améliorée.

Les mécanismes de filtrage peuvent être mis en place à divers endroits de l'architecture globale du Web :

- Ils peuvent être mis en place à titre d'élément du logiciel installé sur le serveur mandataire du FSI. Le logiciel est exécuté sur les sites Web qui ont été extraits par le serveur mandataire ou qui y sont déjà stockés.
- Ils peuvent être exécutés à un niveau plus précis sur l'ordinateur du client à titre d'application autonome ou dans le contexte d'un navigateur standard.
- Ils peuvent résider sur un site Web hôte.
- Ils peuvent être exécutés par un ou plusieurs agents au niveau du serveur.

- Ils peuvent être exécutés par des agents mobiles ou des robots Web.

L'analyse économique coûts/avantages de ces méthodes n'entre pas dans l'objet de ce rapport. Notons cependant que ce genre d'analyse permettrait d'examiner les points suivants :

- Coût de catégorisation proactive des évaluateurs de sites Web de façon continue.
- Coût de stockage et de distribution de cette information.
- Coût de traitement de cette information au moment de la recherche.
- Coût de développement de navigateurs autonomes intégrant des fonctions appropriées.
- Coût de vérification des sites Web, des étiquettes, des listes et des utilisateurs.

Soulignons qu'aucune des technologies mentionnées n'est efficace à cent pour cent et que le contenu du Web est de par nature très volatile. Pour augmenter l'efficacité de ces technologies, il faut les combiner et les utiliser en couches, à la fois au niveau du FSI et au niveau du client.

Les secteurs qui offrent les plus grandes possibilités et sur lesquels on devrait axer les futurs travaux sont les suivants :

- Développement d'architectures qui combinent divers mécanismes permettant de travailler en collaboration ou constituant des couches d'architecture. On pourrait par exemple avoir des étiquettes gérées par un bureau d'étiquettes (Label Bureau), avec des listes gérées par le FSI, l'analyse du contenu étant gérée au niveau du client.
- Recherches plus approfondies en ce qui concerne les robots et les agents Web pour permettre la catégorisation proactive des sites Web.
- Développement d'architectures gérant le filtrage coopératif pour des groupes d'utilisateurs.

Alors que pratiquement toutes les méthodes étudiées dans ce rapport peuvent être mises en œuvre par un FSI, il importe que le filtrage soit transparent pour l'utilisateur. L'utilisateur doit savoir à quel moment le filtrage est en place ou à quelle étape il a eu lieu. Pour que la méthode soit efficace, voici ce qui est importe :

- L'utilisateur doit savoir à quelle étape le contenu a été filtré et la raison pour laquelle il a été filtré.
- L'utilisateur doit connaître les critères de filtrage, c'est-à-dire ce qui figure sur la liste ou dans le filtre.

Compte tenu de la nature dynamique du Web, il faudra axer les efforts, de façon concertée et soutenue, sur le développement, l'évaluation et la maintenance de mécanismes de filtrage et de contrôle d'accès, et ce, à tous les niveaux - gouvernement, collectivité, FSI et utilisateurs individuels.

## Annexe

### Exemples de logiciels de filtrage

La liste présentée à la page suivante donne des exemples de logiciels de filtrage[45] utilisant quatre mécanismes de contrôle.

- Domaine sûr—recommander du contenu adéquat pour les enfants.
- Recherche—sélectionner du contenu qui soit adéquat pour les enfants et qui concorde avec la requête.
- Surveillance—enregistrer, en vue d'une inspection ultérieure, une liste des documents auxquels l'utilisateur a accédé ou a tenté d'accéder.
- Blocage—empêcher les enfants d'accéder au contenu.

Remarquez que la technologie de base qui est de loin la plus utilisée est le blocage à l'aide des étiquettes, des listes d'URL ou de l'analyse du texte et que la plupart des systèmes font appel à plus d'une technologie.

[45] Cranor, Lorrie Faith, Danielle Gallo et Paul Resnick. (1998*). Technology inventory: a catalog of tools that support parents; ability to choose online content appropriate for their children.* [En ligne]. DFSIonible à : http://www.research.att.com/projects/tech4kids/index.html [janvier 2000]

| N° | Logiciel | Domaine sûr | Recherche | Surveillance | Blocage |
|---|---|---|---|---|---|
| 1 | Access Management Engine (AME) | X | | | X |
| 2 | AltaVista Filtered Search Service | | X | | |
| 3 | America Online Parental Controls | | | | X |
| 4 | Bess | | | X | X |
| 5 | Bonus.com the SuperSite for Kids | X | | | X |
| 6 | ChoiceView | | | X | X |
| 7 | Click and Brose Jr. | X | | | X |
| 8 | Cyber Patrol | X | | | X |
| 9 | CYBERsitter | | | X | X |
| 10 | Cyber Snoop | X | | X | X |
| 11 | Disney's Blast Online | X | | | X |
| 12 | EdView | X | X | | X |
| 13 | ESRB | | | | X |
| 14 | evaluWEB | | | | X |
| 15 | GuardiaNet | | | X | X |
| 16 | I-Gear | | | X | X |
| 17 | IBM Web Traffic Express | | | | X |
| 18 | The Internet Filter | | | X | X |
| 19 | The Internet Kids & Family Yellow Pages | X | | | |
| 20 | KidDesk Internet Safe | X | | | X |
| 21 | Kids CyberHighway | X | | | X |
| 22 | Mail Gear | | | X | X |
| 23 | Mayberry USA | | | X | X |
| 24 | Microsoft Internet Explorer | | | | X |
| 25 | NetFilter | | | | X |
| 26 | Net Nanny | | | X | X |
| 27 | Net Rated | | | X | X |
| 28 | Netscape 4.5 | | | | X |
| 29 | Net Shepherd | | X | | X |
| 30 | PlanetView | | | | X |
| 31 | RSACi | X | X | X | X |
| 32 | SafeSurf | X | X | X | X |
| 33 | Scholastic Network | X | | | |
| 34 | SmartFilter | | | X | X |
| 35 | SurfWatch | | | | X |
| 36 | WatchGuard SchoolMate | | | | X |
| 37 | WebChaperone avec iCRT | | | X | X |
| 38 | WebDoubler | | | X | X |
| 39 | WebSENSE | | | X | X |
| 40 | WinGuardian | | | X | |
| 41 | X-STOP | | | | X |

**Tableau 3. Logiciels de filtrage et mécanismes de contrôle qu'ils utilisent**